UNIVERSIDAD CARLOS III DE MADRID
Departamento de Ingeniería Telemática

PROYECTO FIN DE CARRERA

Análisis teórico-experimental de técnicas y herramientas de phishing y delitos electrónicos

Autor: Abel Lozano Prieto

Tutor: Francisco Valera Pintor

Leganés, octubre de 2009

Título: Análisis teórico-experimental de técnicas y herramientas de phishing y delitos electrónicos
Autor:
Director:

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Llegado este momento tan importante en mi vida, no puedo olvidarme de agradecer a todas las personas que me han ayudado a lo largo de todos estos años. Sin su apoyo, hubiera sido más difícil llegar hasta donde estoy.

Quiero dar las gracias a mis padres, Abel y Lina, que en esta etapa universitaria han soportado con mayor o menor paciencia y a su manera mis preocupaciones y que sin duda han contribuido a alcanzar este final, animándome cuando lo he necesitado.

A Irene, por la atención que siempre me ha dispensado y sobre todo, que cuando las cosas se ponían más complicadas, ha estado a mi lado dándome todo su apoyo. Gracias por poder contar siempre contigo.

A mi hermana Raquel y a mi familia, especialmente a mi abuelo Feliciano, que siempre ha estado pendiente de mi carrera y quería que su nieto fuera ingeniero desde que era bien pequeño: ya lo tiene. También quiero recordar a mi abuela Adelina, que sin duda, hubiese disfrutado al verme llegar hasta aquí.

A mis compañeros de la universidad: Aynos, Gordi, Juárez, Luisma, Muñoz, Santi, Sergio y muchos más, por los buenos y malos momentos que hemos pasado juntos, siempre dispuestos a ayudarnos entre todos y por tantas horas de clases, prácticas, cafetería y laboratorios haciéndonos la carrera un poco más llevadera. Especialmente a Agus, que durante los dos últimos cursos hemos compartido todas las horas de estudio y universidad, y con cuya compañía la recta final ha sido mucho más fácil. A Julio, que aunque llegó antes a la meta, no perdimos el contacto y siempre ha estado a mi lado brindándome su apoyo y amistad. Y a Paco, por todas las “aventuras extrauniversitarias” (biblioteca, viajes, empresas que hemos organizado,…) que nos han mantenido unidos y que siempre contará conmigo.

También quiero agradecer el trabajo y esfuerzo que me han dedicado mis dos tutores: Francisco Valera en la Universidad, siempre dispuesto a resolver mis dudas con prontitud y rapidez. A Juan Carlos G. Cuartango, que desde el primer momento y desinteresadamente me acogió en su empresa, Instisec, brindándome todo su apoyo, su experiencia y su tiempo. Sin duda alguna su orientación ha sido valiosa para la realización de este proyecto.

Imposible es solo una palabra que usan los hombres débiles para vivir fácilmente en el mundo que se les dio, sin atreverse a explorar el poder que tienen para cambiarlo. Imposible NO es un hecho, es una opinión. Imposible no es una declaración, es un reto. Imposible es potencial. Imposible es Temporal, "Imposible is nothing"

Mohamed Ali

Resumen

El comienzo de la *era Internet* supuso un cambio radical en la información, comunicación, servicios, ocio y en la vida en general de nuestra sociedad. La evolución de todo lo que ofrece la *red* crece constantemente. Al igual que el resto de sectores, el mundo de la *banca* ha ido aprovechando lo que las comunicaciones electrónicas pueden ofrecerle.

La *banca electrónica* brinda muchas comodidades a los clientes, permitiéndoles consultar saldos, realizar transferencias, invertir en bolsa e incluso dar de alta nuevas cuentas y depósitos desde su propio hogar. Los bancos también tienen beneficio: enorme reducción de trabajo en las sucursales, mayor número de contrataciones de depósitos e inversiones debido a la comodidad que esto supone, mejor comunicación con los clientes, etc.

Pero al igual que todo avance presenta ventajas, siempre pueden surgir inconvenientes. Al ser estos servicios a distancia y por ello, no ser necesaria la presencia del actor, las comunicaciones siempre pueden llegar a ser interceptadas, las identidades suplantadas y las acciones no supervisadas por una persona física. Todo esto genera nuevos horizontes para los delincuentes, que evolucionan a la par que la sociedad y actualizan sus métodos, muchas veces de forma más rápida que el propio sector de servicios.

En este proyecto se ha estudiado el estado actual de la delincuencia electrónica, en qué medida afecta a clientes y empresas, se han analizado las múltiples tecnologías que emplean y buscado soluciones para anular estos ataques.

Índice general

Índice de figuras

Capítulo 1

Introducción

1.1 Introducción

Cada año crece considerablemente el número de víctimas de estas estafas, así como la complejidad de las mismas. Concretamente en el mundo bancario, los delitos aumentan de forma exponencial.

La evitación de los delitos depende de:

- Soluciones de diseño y tecnológicas: engloban el diseño de sistemas operativos, navegadores web, servidores de correo electrónico, sistemas de seguridad y cifrado, procedimientos de validación, diseño de páginas de banca electrónica, etc.
- Información y concienciación del usuario final.

Estos elementos involucrados suponen un gran problema a la hora de evitar los ataques phishing y permiten a los delincuentes tener tiempo suficiente para ir siempre un paso por delante.

En el ámbito de la ingeniería civil, cualquier tecnología desarrollada en la actualidad o en el pasado está documentada y la mayor parte es fácilmente accesible por los profesionales del sector. El gran problema que existe es que la tecnología y métodos empleados en el mundo de los delitos informáticos, son muy desconocidos para la mayoría. Esto sucede porque con estos delitos se persiguen fines ilegales y al ser usados únicamente por personas que no quieren que se descubra cómo han sido desarrollados y

utilizados, no habrá ninguna documentación sobre los mismos. Por ello, se va a requerir de una gran labor de investigación para poder dar luz sobre ellos.

Este proyecto no es un proyecto al uso, pues además de tener una parte técnica, también tiene una gran labor de investigación en ámbitos más allá de lo tecnológico. Gran parte de esta ha consistido en introducirse personalmente en el mundo del *phishing*, contactando directamente en foros con personas que se dedican a ello y buscando formas de ser atacados para estudiar las herramientas que se usan. Por lo tanto una porción considerable del tiempo utilizado se ha dedicado a seguir pasos similares a los que realiza la policía científica y el periodismo de investigación.

Esta labor de investigación ha supuesto una dedicación constante debido a la espera continua de captación de material directamente del mundo real, al desecho de un gran porcentaje de muestras no válidas después de haber sido estudiadas profundamente, ya sea por haber caducado o por quedar fuera de los objetivos del proyecto y a la necesidad de realizar los estudios con rapidez, puesto que en el mundo de los delitos electrónicos, el periodo de vida de las herramientas es de horas.

Muchos de estos resultados no hubieran sido posibles sin la estrecha colaboración mantenida con la empresa Instisec y con su director, Juan Carlos García Cuartango, tanto por las herramientas que han puestos a nuestro alcance, como el conocimiento impartido sobre los delitos tecnológicos y de seguridad en la red.

1.2 Objetivos

Debido a la naturaleza ilegal de los delitos informáticos, existen muy pocos documentos sobre los medios que se utilizan. No sólo la información es mínima, sino que además está dispersa y es confusa.

El objetivo principal de este proyecto es la caracterización de medios y herramientas usados en el mundo de los delitos bancarios.

Para ello se han decidido los principales pasos a seguir:

- Análisis de la escuela brasileña
- Análisis de la escuela rusa
- Análisis de captación de *mulas*

A lo largo de la investigación se irán examinando diferentes muestras de correos electrónicos phishing, páginas web phishing y malware usado actualmente por los delincuentes, definiendo los siguientes subobjetivos:

- Estudio de envío y recepción de correo *spam*
- Captación y estudio de correos electrónicos *phishing*
- Estudio de páginas web *scam*
- Captación y recopilación de muestras de *malware*
- Estudio detallado de muestras de *malware*
- Captación y estudio de correos electrónicos de *muleros*

Una vez estudiada toda la información, se presentarán conclusiones sobre seguridad orientadas tanto a programadores y entidades financieras como a usuarios finales.

1.3 Medios con los que se ha contado para la realización del proyecto

Para la realización del proyecto se han necesitado ayudas externas de empresas de seguridad que han ofrecido su colaboración dotando de software especializado, muestras de malware actual y recomendaciones muy útiles.

Se han utilizado los siguientes medios:

Software:

- Servidor de correo: Argosoft Mail Server [1]. Utilizado para el estudio, recepción y caracterización de correos spam.

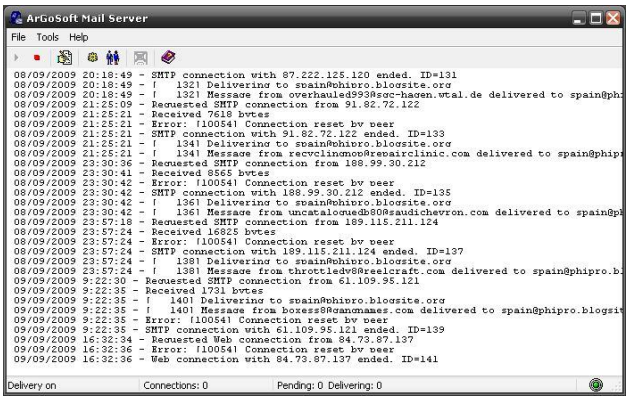


Figura 1. Argosoft Mail Server

- Gestor de máquinas virtuales: VMWare Workstation [2]. Necesario para la ejecución y estudio de muestras de malware sin poner en peligro la integridad del equipo o los datos del usuario.

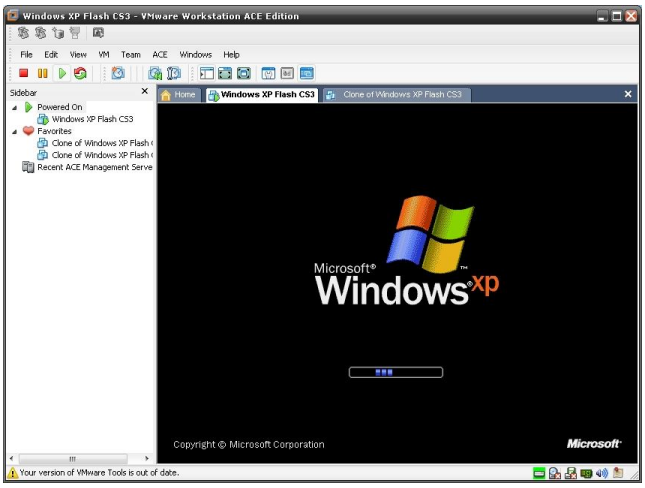


Figura 2. VMWare

- Analizador de instalaciones: Install Watch Pro [3]. Hace un listado de todas las tareas realizadas por la instalación de un programa en un equipo, muy útil.

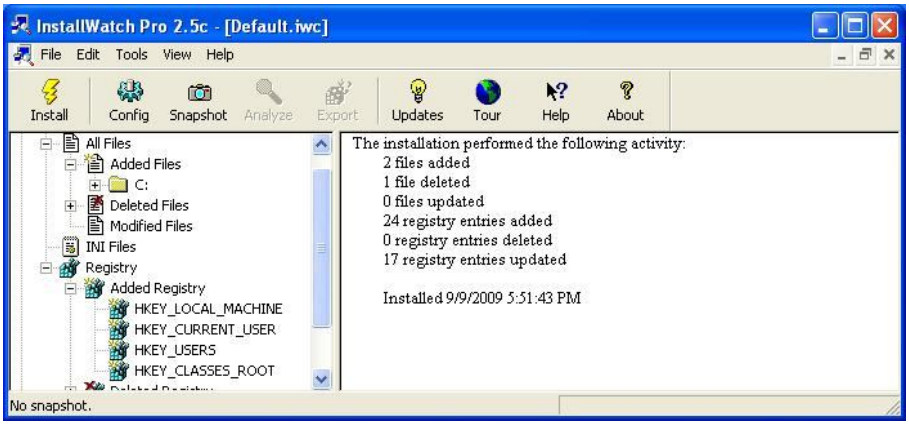


Figura 3. Install Watch Pro

- Analizador de redes: Wireshark Network Analyzer [4], eEye Iris Professional [5]. Usado para monitorizar todos los paquetes emitidos y recibidos por un equipo a la hora de estudiar las transacciones de información que ocurren con la ejecución de malware y comunicaciones de elementos phishing.

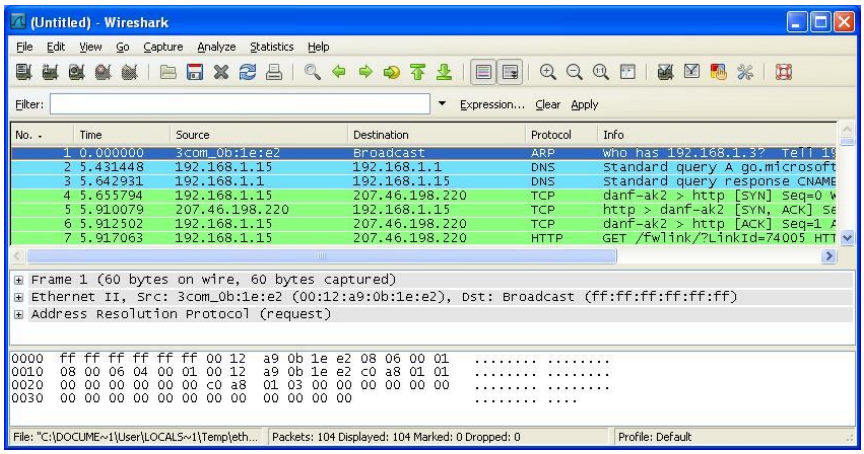


Figura 4. Wireshark

- Registro ficheros: File Monitor [6]. Permite visualizar el acceso a ficheros por el sistema operativo para ver qué tareas realiza una muestra de malware a estudiar.

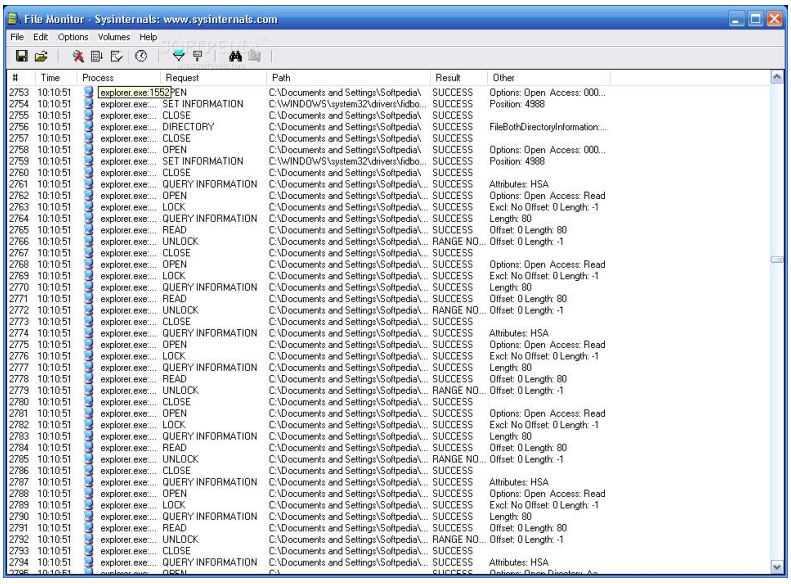


Figura 5. Filemonitor

- Registro procesos: Process Explorer [7]. Útil para controlar los posibles subprocesos creados por el malware.

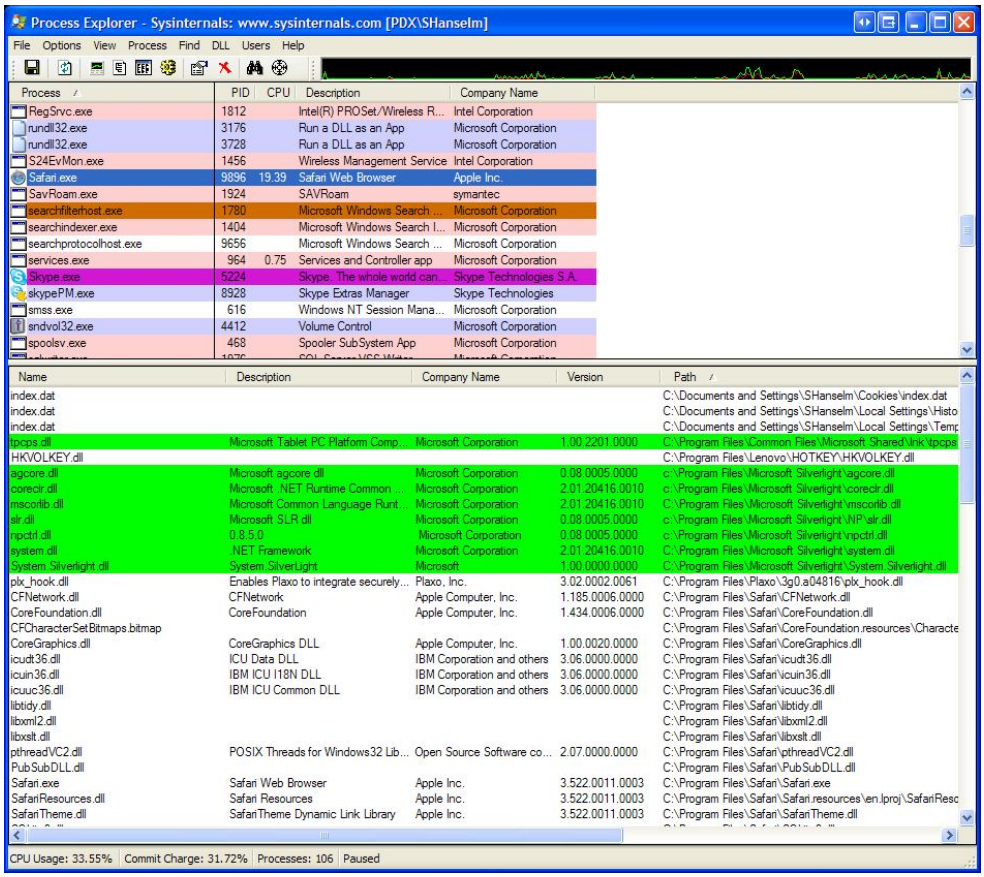


Figura 6. Process Explorer

- Motores de búsqueda de virus: Virus Total [8]. Se ha empleado para una primera caracterización.

Figura 7. Virus Total

Servicios:

- Proveedores de malware y herramientas de análisis: Instituto Seguridad Internet, Hispasec Sistemas.

Empresa Instituto Seguridad Internet

Este proyecto se ha realizado con la ayuda de la empresa Instisec y su director, Juan Carlos García Cuartango, posiblemente el profesional más prestigioso del sector de la seguridad en Internet en España. Su prestigio le ha llevado a salir en diferentes publicaciones y a participar en Congresos y seminarios como experto en seguridad.

En esta empresa se han adquirido conocimientos sobre el mundo del Phishing y el uso de herramientas para la detección y análisis de delitos electrónicos, así como recomendaciones y tutorías para el buen progreso del estudio.

Esta empresa también ha puesto a nuestro servicio máquinas para alojar servidores y dominios de correo y muestras de malware de última generación que les hacen llegar diariamente desde diversas entidades de seguridad.

1.4 Estructura de la memoria

1.4.1 Estado del arte

Hace referencia a los conocimientos que se tienen en la actualidad sobre delitos electrónicos. Introduce el concepto de *phishing bancario*, habla sobre las dos escuelas principales y muestra las diferentes fases que se utilizan para la consecución del robo de dinero. Toda esta información se ha recopilado investigando la poca y dispersa documentación que existe al respecto y con ayuda de los conocimientos impartidos por Juan Carlos García Cuartango en Instisec.

1.4.2 Análisis teórico-experimental

Una vez realizada la recopilación de información sobre el tema a tratar, se pasó a decidir con ayuda de los tutores tanto en la universidad como en Instisec las pruebas a desarrollar para cumplir los objetivos del proyecto. El análisis teórico experimental ha estudiado los siguientes temas:

- Captación de direcciones de correo electrónico
- Correos electrónicos *phishing*
- Páginas *web scam*
- Malware
- Otras herramientas *phishing*
- Muleros

1.4.3 Conclusiones y trabajo futuro

A partir de las pruebas realizadas y del análisis de los datos obtenidos se han recopilado un conjunto de conclusiones y recomendaciones para temas de seguridad a distintos niveles. También se trata el trabajo futuro que se podría hacer a partir del final de este proyecto; cómo continuar el estudio con otras pruebas disponiendo de más tiempo y en algunos apartados, más medios.

1.4.4 Presupuesto

Muestra las distintas fases del proyecto, cómo se han repartido tiempo y recursos para estas y los gastos económicos asociados.

Capítulo 2

Estado del arte

2.1 Qué es phishing

Phishing es un término que se refiere a un tipo de estafa cuyo fin es la obtención de información confidencial de interés para el estafador [9]. Comúnmente estos datos son credenciales bancarias (nombres de usuario, contraseñas de acceso, claves de operación, números de tarjetas de crédito, etc). Para obtener esta información se hace uso de ingeniería social [10].

El estafador, conocido como phisher, se hace pasar por una entidad de confianza y establece una comunicación con la víctima, haciendo que esta le proporcione los datos buscados.

El origen del término proviene de la palabra inglesa “fishing”, haciendo alusión a la “pesca” que se hace con las personas estafadas. El cambio de ‘f’ por ‘ph’ es algo muy común en el mundo hacker [11]. Todo empezó con el primer movimiento hacker de la historia, el “phreaking” [12] (proveniente de “phone” y “freak”).

2.2 Escuelas

Los delincuentes pueden usar métodos variados para la captación de datos de usuarios. Estas metodologías se dividen fundamentalmente en dos escuelas [13]:

2.2.1 Escuela brasileña

Se centra en el uso de ingeniería social para la obtención de datos. Su fin es conseguirlos directamente de la mano del usuario estafado. Para ello realizan una suplantación de identidad de la entidad bancaria y contacta con el usuario usando razones variadas para que éste les proporcione los datos que buscan. El método de contacto por excelencia es el envío masivo de correos electrónicos a la espera de que se dé la situación de coincidencia de un usuario que sea cliente de la misma entidad que la que los delincuentes simulan ser, y que éste caiga en la trampa. La probabilidad a priori de enviar un email haciéndose pasar por un banco en particular, que el destinatario sea cliente de ese banco, crea a su vez en la procedencia del correo y actúe en consecuencia, es bastante baja. La solución a esto, consiste en el envío indiscriminado de mensajes no solicitados, suplantando identidades de múltiples bancos y usando listas de correo de millones de direcciones. El atacado puede dar sin saberlo los datos directamente o infectar manualmente su ordenador para que los atacantes puedan obtenerlos más adelante.

2.2.2 Escuela rusa

La escuela rusa es bastante más peligrosa para el usuario que cree no caer en las trampas de la escuela brasileña, pues la obtención de datos no usa la ingeniería social, sino las vulnerabilidades de seguridad de los portales de banca, de protocolos de red, e incluso de sistemas operativos.

2.3 Captación de la información

La captación de información se puede dar de múltiples maneras. Vamos a introducir y desarrollar los métodos partiendo de los más sencillos hasta los más elaborados tecnológicamente.

2.3.1 Algunas técnicas usadas

2.3.1.1 Páginas web falsas

Consiste en una imitación de la página web oficial de la entidad. Para conseguir que los atacados accedan a ella en vez de a la verdadera, se hace uso de un link en los correos de spam (escuela brasileña) o a través de la modificación de las direcciones dns del

sistema o la infección del navegador web (escuela rusa). Estas webs presentas ciertas características que se estudiarán más adelante.

Figura 8. Caja Madrid

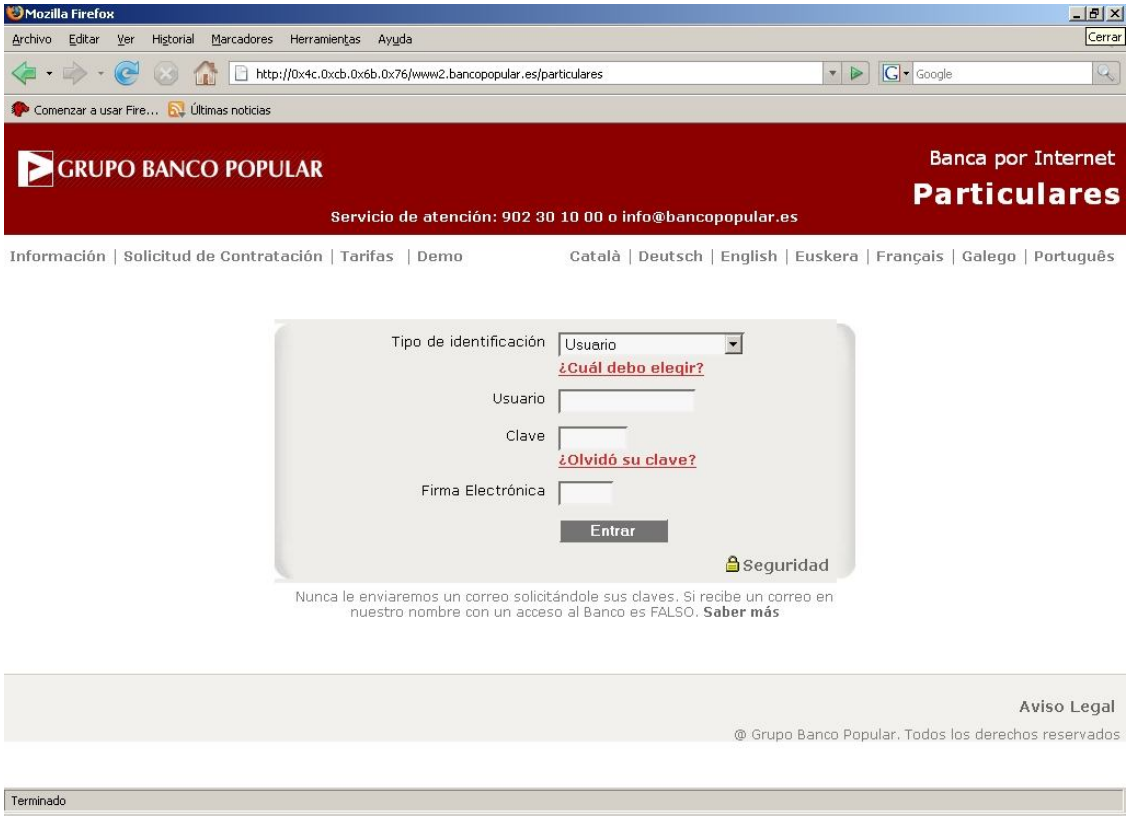


Figura 9. Banco Popular

2.3.1.2 Introducción directa de malware

El atacante consigue que ya sea adjuntándolo en un correo electrónico o descargándolo de una web, la víctima ejecute un archivo que contenga un programa encargado de obtener datos personales, ya sea de forma directa o indirecta.

2.3.1.3 Man-in-the-middle

El atacante se sitúa en medio de la comunicación cliente-entidad haciendo de proxy entre ambos. De esta forma, el cliente cree estar conectado directamente a la entidad y la entidad directamente al cliente. Para que este esquema sea posible, se requiere de otras técnicas como proxies transparentes, inyección de HTML, DNS Poisoning u ofuscación de URLs.

Este tipo de ataque permite procesar los datos en tiempo real.

2.3.1.4 Vulnerabilidades Cross-Site Scripting

Simulan una página web bancaria segura, manteniendo a simple vista el certificado de la entidad y la URL de la página

2.3.1.5 Vulnerabilidades del navegador web

Falsean la dirección que aparece en la barra de direcciones a través de software o secuencias de comandos que se aprovechan de errores de programación. Así se puede visitar una página web fraudulenta mostrandose la dirección real. Esto permite también falsear las ventanas pop-up de la entidad bancaria.

También se puede infectar un equipo a través de estas vulnerabilidades una vez se visita una página web que tenga contenido fraudulento y aproveche estos agujeros para introducir troyanos.

2.3.1.6 Pharming

Consiste en cambiar los contenidos DNS (Servidor de Nombres de Dominio) a través de la configuración del protocolo TCP/IP o de la caché local de nombres de servidores *lmhost*. De esta forma al teclear la dirección web del banco, la IP de respuesta a la consulta DNS será la de una web falsa.

2.3.1.7 Man-in-the-endpoint

Este tipo de ataque constituye en gran medida el futuro del mundo de los delitos informáticos. Al contrario que los ataques de tipo *man-in-the-middle*, no necesitan servidores adicionales para interceptar el tráfico entre el cliente y el servidor, ya que todas las modificaciones se realizan en el sistema local. Por el contrario, requiere mucho más esfuerzo y tiempo por parte del delincuente debido a que para que este sistema funcione, el equipo debe estar infectado con un troyano que capture el tráfico HTTPS.

Estos troyanos normalmente son capaces de recibir órdenes desde un servidor de control que guarde credenciales y cantidades de dinero a transferir, de forma que se puede enviar información al ordenador infectado para que este transfiera fondos a una cuenta destino como si lo estuviera haciendo el propio dueño del equipo y de la cuenta.

2.4 Distribución de ataques por correo electrónico

2.4.1 Introducción

El correo electrónico es un medio rápido, cómodo y económico para llegar a las personas. La automatización de envíos y la adquisición de enormes listas de direcciones hacen posible el envío de información a millones de personas usando medios muy escasos. Esto hace que sea el medio ideal para realizar ataques con el fin de obtener datos personales.

Las principales razones del envío y recepción de correo no deseado son:

- **Publicidad fraudulenta:** comúnmente conocido como spam. Ofertas de productos y servicios, tanto legítimos como ilegítimos. Un claro ejemplo de este tipo de correos es la venta de medicamentos.
- **Recopilación de direcciones de correo:** la creación de cadenas a partir de noticias falsas y bulos, en las que se busca el reenvío de los correos a todos los contactos de los usuarios representa una buena baza para los recopiladores de direcciones, puesto que la expansión es inmediata y de progresión geométrica. Normalmente se suele incluir una amenaza de desgracia en caso de no reenviarlo, para así meter más presión al que lo lee a la hora de reenviarlo. En el texto del correo quedan incluidas las direcciones de todos los reenvíos que se han realizado desde el principio, y una vez llegan de vuelta estas cadenas a manos de los interesados, suponen una fuente inmensa de direcciones que les servirán para proceder a envío de spam o la comercialización de éstas.
- **Fraude económico directo:** envío de correos phishing con la intención de obtener las credenciales bancarias de las víctimas para el posterior robo de dinero de sus cuentas.
- **Diseminación de malware:** en forma de archivos adjuntos. Normalmente el texto del correo anima de cierta forma al usuario a ejecutar el archivo, ya sea mostrándolo como algo divertido o una sorpresa. De esta forma el propio usuario infecta su equipo directamente, normalmente con malware encargado de robar credenciales, aunque los objetivos pueden ser otros que estudiaremos más adelante.

Para la escuela brasileña, el envío de phishing es básico. Aunque se puede afirmar que con el paso del tiempo va existiendo una concienciación de los usuarios sobre la posibilidad de recibir correos falsos supuestamente de entidades fiables, por muy

pequeño que pueda llegar a ser el porcentaje de los susceptibles de caer en el engaño, un envío indiscriminado de éstos asegura una cantidad aceptable de víctimas.

La escuela rusa también hace uso de este medio, ya que es una buena forma de diseminar malware que les permita obtener estos datos que buscan de forma directa y también de forma indirecta, abriendo puertas traseras en los equipos de los atacados para realizar ataques de otro tipo en un futuro.

2.4.2 Redes Botnet

Debido a que el envío de estos correos no deseados es ilegal y fácilmente rasteable, el sistema usado para enviarlos consiste en infectar cientos de ordenadores con malware y usarlos para todo el proceso de spam. Estos equipos infectados, conocidos como *zombies*, se unen formando redes llamadas *botnets* que son comandadas desde un equipo principal controlado por el infractor. La capacidad de estas redes es grandísima, debido a que el conjunto de equipos trabaja como uno solo, de forma que la actuación está distribuida. Esta distribución hace que la velocidad de red y de computación equivalentes sean extremadamente altas y permiten realizar acciones que serían inviables desde un solo equipo o una red pequeña. Esta distribución también hace que la detección y bloqueo de ataques sea prácticamente imposible.

El hecho de que sea una red distribuida, presenta dos ventajas principales al administrador de la *botnet*:

- Al estar descentralizada es prácticamente imposible parar su funcionamiento, puesto que son miles de equipos funcionando al unísono, y eliminar varios de ellos no supone ningún problema para el funcionamiento global.
- La capacidad total de procesamiento es muy elevada, puesto que son miles de ordenadores trabajando en paralelo, cada uno haciendo uso de sus recursos y de su red propia. De esta forma, el rastreo de direcciones y el envío de correos no plantean problemas de congestión de red.
- Estas redes permiten a su administrador realizar todos los pasos necesarios para lograr el proceso del envío de correo no deseado, gestionando este las tareas que tienen que realizar los equipos zombies, ya sea de forma manual o automatizándolo:
- Búsqueda de direcciones de correo válidas:
  - Rastrear la web en busca de direcciones de correo
  - Enviar correos electrónicos para comprobar su correcta entrega o directamente establecer un enlace SMTP con el servidor de correo del dominio de la dirección a estudiar con el objetivo de chequear la validez de una dirección de correo
  - Remitir al equipo del administrador las direcciones válidas que se van procesando
- Envío masivo de correos no deseados: los equipos zombies actúan también como servidores de correo, usando estas direcciones de correo válidas como destinatarios. Un ejemplo de ello es la Botnet Ron Paul. [14]

La mayoría de las veces los equipos se infectan de forma manual por el usuario. En plataformas Windows, es muy común instalar programas descargados de Internet que

dentro de su código también contienen *bots* que se autoejecutan y consiguen que el equipo quede infectado.

Además de esto, los equipos *zombie* también pueden infectar por distintos métodos otros equipos con el objetivo de ampliar la capacidad de la *botnet*, ya sea enviando correos electrónicos infectados, o con subprogramas que aprovechan vulnerabilidades de otros equipos conectados a la red.

Los códigos maliciosos que infectan los equipos suelen estar contenidos en programas gratuitos y en generadores de claves y números de serie. Rara vez son detectados por programas antivirus.

Dado que las redes botnet trabajan de forma oculta y su objetivo nada tiene que ver con el usuario del equipo infectado, la detección por parte de éste de que su ordenador forma parte de una red fantasma es complicada. Los pocos indicios que se pueden tener es comprobar que el número de conexiones es muy elevado y que el rendimiento del ordenador puede ralentizarse.

Existe un mercado de redes *botnet* en el que los administradores o dueños de una red de este tipo, alquilan sus servicios a *spammers* durante un tiempo a cambio de dinero.

La razón de ser principal de este tipo de redes es su uso para el bombardeo de correo no deseado, pero también son usadas en algunas ocasiones para robar información bancaria, diseminar programas espía o realizar ataques DDoS (Distributed Denial of Service).

2.4.3 Captación de direcciones

2.4.3.1 Introducción

Los sistemas de captación de direcciones de correo para su posterior explotación en el envío masivo no están muy estudiados.

Las posibles técnicas de captación de direcciones principales son las siguientes:

- Rastreo web: las direcciones de correo que pueden aparecer en páginas web, foros, blogs, etc, pueden ser rastreadas por bots programados para ello y guardadas en enormes bases de datos que luego se pueden utilizar para el envío de spam o incluso comercializar. Existe un “mercado negro” de datos de usuarios bastante amplio.
- Mensajes en cadena: como se ha explicado anteriormente, una vez recibe el interesado un mensaje de cadena, en el cuerpo de éste puede obtener cientos de direcciones de correo válidas.
- Uso de malware: existen programas maliciosos que al ser ejecutados en un equipo, entre otra información de interés, obtienen direcciones de correo de los emails almacenados y de las libretas de de contactos y posteriormente las envían al interesado.
- Programas que generan nombres aleatorios y envían correos a algunos dominios de forma que cuando no reciben un mensaje de error, detectan que es una dirección válida.

- Rastreamiento de grupos de noticias y listas de correo. De esta forma se pueden obtener grupos de direcciones cualificadas.
- Formularios de solicitud de información contenidos en páginas web que piden datos para dar una cuenta de alta o para ofrecer algún servicio a cambio. Estos datos pueden ser objetivo de uso fraudulento.

2.5 Escuela brasileña

2.5.1 Introducción

Como ya se ha comentado anteriormente, la escuela brasileña se basa en el uso de la ingeniería social [15]. Establece un contacto directo con la víctima haciéndose pasar por una entidad bancaria fiable, sin usar vulnerabilidades o infecciones con malware.

Este establecimiento de comunicación se produce gracias al envío masivo de correos electrónicos que requieren la actuación del usuario víctima. Para que el engaño funcione, es necesario que se cumpla a la vez

- Que el correo recibido se catalogue como correo deseado por el servidor de correo y por el propio destinatario.
- Que el destinatario sea cliente de la entidad que el correo simula ser.
- Que el destinatario confíe en el contenido del correo.
- Que el destinatario siga los pasos que el correo le indica.

Como puede observarse, esta lista de condiciones es bastante extensa, y la probabilidad de que se cumplan todas para que el engaño se realice es ínfima.

No obstante, este bajo rendimiento se suple con un número descomunal de intentos de ataque; siendo el espacio muestral muy amplio, aún con una probabilidad de éxito baja, se puede obtener un resultado bastante positivo en cuanto a ataques logrados. Con la obtención de los datos personales de muy pocas personas se pueden conseguir unos beneficios económicos muy cuantiosos.

Una vez se ha conseguido que la víctima crea en la veracidad del correo, se le pide que siga unas instrucciones con el objetivo de obtener sus credenciales. Normalmente se le solicita pinchar sobre un enlace que lleva a una página web falsa del banco y posteriormente que introduzca todos sus datos. En otras ocasiones, el enlace lleva a la descarga de una aplicación o directamente esta viene adjuntada en el correo. Esta aplicación tiene la misma funcionalidad que la web falsa, ya que recoge los datos que el usuario introduce aunque con la diferencia de que el phisher no tiene que montar un servidor web y de esa forma su rastreo por las fuerzas del orden será mucho más complicado.

Todas estas comunicaciones se excusan en la necesidad de confirmar los datos del usuario o de reactivar su cuenta debido a supuestos intentos fallidos de conexión o a nuevas actualizaciones de seguridad de la entidad.

2.5.2 Ingeniería social

El término fue popularizado por Kevin Mitnick, uno de los primeros hackers de la historia. Afirma que el factor más importante de la seguridad de las redes no es el software ni el hardware de estas, sino la capacidad de sus usuarios de interpretar las políticas de seguridad y de hacerlas cumplir.

Consiste en el uso de engaños y manipulaciones para que alguien revele datos confidenciales o realice alguna acción. Su uso supone una debilidad universal en el ámbito de la privacidad, ya que cualquier persona con el acceso a alguna parte del sistema, física o electrónicamente, es un riesgo potencial de inseguridad. [16]

Los principios de los que se vale la ingeniría social, según Mitnick son [17]:

- Todos queremos ayudar.
- El primer movimiento siempre es de confianza hacia el otro.
- No nos gusta decir “no”.
- A todos nos gusta que nos alaben.

Estos principios hacen que las técnicas de ingeniería social sean extremadamente eficaces y que formen la base de la escuela brasileña.

Los métodos utilizados son dos:

- **Demanda directa**: a la víctima se le pide abiertamente la información o realizar una tarea. Es la forma más fácil y sencilla, ya que sabe lo que el remitente quiere que haga.
- **Demanda indirecta**: se idea una situación de la que forma parte la víctima y se le plantea. Si cree en las razones que se le plantean, el éxito está asegurado.

Contrariamente a lo que cabe esperar, en la mayor parte de los casos, es más cómodo y eficaz utilizar a las personas que aprovechar agujeros de seguridad de los sistemas. Las vulnerabilidades tecnológicas siempre pueden ser reparadas, pero las personas nunca dejarán de ser vulnerables. [18]

2.5.3 Correos electrónicos

Después de estudiar con detenimiento decenas de correos *phishing*, se puede concluir que tienen ciertas características comunes que mostraremos a continuación.

Estos mensajes presentan propiedades que les pueden hacer difícil de demostrar su no legitimidad:

- **Campo “De:”:** muchos clientes de correo permiten elegir el nombre del emisor del correo, así como su dirección de origen (tanto usuario como dominio). De esta forma no es ningún problema que hacer que el remitente pertenezca al mismo dominio que la entidad bancaria en cuestión.
- **Imágenes y logotipos oficiales:** al ser estas imágenes públicas y de fácil acceso, se incluyen los logotipos de la empresa en el cuerpo del correo. Simplemente consiste en copiarlas de la página web oficial.

- **Personalización:** en ocasiones los mensajes son personalizados e incluyen en el texto el mismo nombre de usuario que el mail destino. Esto puede hacer creer al destinatario que efectivamente le están contactando de forma personal y que el correo no pertenece a un envío masivo.

De la misma forma, hay otras propiedades que pueden hacer factible la detección de su falsedad:

- **Uso del lenguaje:** de los mensajes estudiados, el 95% del total presentan errores gramaticales, ortográficos y sintácticos bastante llamativos. Los delincuentes intentan atacar a personas de diferentes países y no tienen medios como para contratar traductores profesionales. La traducción de los mensajes normalmente proviene de traductores web automáticos, por ejemplo Google Translate.
- **Links:** los links que presentan son misteriosos. Nunca parece que vayan a llevar a un sitio que tenga que ver con la propia entidad. Para disimularlos, muchas veces el link es una imagen con un acceso directo, o incluso una línea de texto con la URL original del banco, que realmente es un hipervínculo a una dirección completamente diferente.

2.5.4 Páginas web

Si el correo electrónico consigue pasar todas las fases para aceptarse como válido, el usuario pulsará sobre el link que le indican. En el caso de llevar a una página web falsa (también llamada "*Scam*"), esta presentará ciertas diferencias no fácilmente visibles por un usuario engañado.

2.5.4.1 Contenido

El contenido de la página web normalmente es similar al original. Los delincuentes no tienen necesidad de desarrollar nada, puesto que directamente copian el código HTML de la página original e introducen pequeñas variaciones, básicamente en modificar las direcciones de envío de datos y en introducir nuevos campos para rellenar con datos o algún aviso de seguridad que refuerce la credibilidad del contenido del correo electrónico.

Los enlaces comunes de este tipo de páginas, como pueden ser contacto, productos, servicios, privacidad, etc, se suelen mantener intactos de forma que el usuario pueda acceder a ellos y le lleven a los originales.

2.5.4.2 Dirección URL

Un navegador web siempre muestra en su barra de direcciones la URL donde nos encontramos. Si no se modifica el programa, la solución para evitar sospechas del usuario es el uso de herramientas para confundirlo. [19]

- **Nombre ligeramente modificado:** cabe la posibilidad de que el una pequeña variación del nombre del dominio de la web bancaria esté sin registrar. En ese caso sería muy poco costoso registrarlo y utilizarlo como dirección original. Basta con la supresión de una letra o la adición de guiones entre palabras.

Normalmente las entidades bancarias registran algunas variaciones de los dominios para evitar estos casos.

Figura 10. Nombre modificado

También existen dominios que incluyen el nombre de la entidad

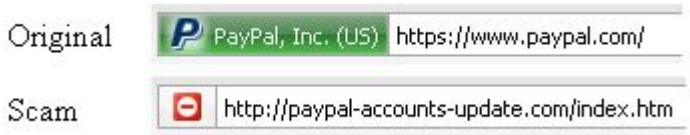


Figura 11. Nombre modificado 2

- **Uso de subdominios:** incluir la dirección del banco en la dirección de la web de phishing: http://nombredelbanco.com.servidorphishing.com. A pesar de ser muy diferente la URL a la original, el simple hecho de ver el nombre de la dirección oficial del banco hace que muchos usuarios den por hecho que la dirección es válida. Este sistema puede ser muy interesante, ya que el abanico de extensiones posibles de dominios es muy amplio. De esta forma se puede registrar prácticamente cualquier nombre de dominio y elegirlo de forma que complemente a la perfección el subdominio elegido. Por ejemplo, si la razón que se da en el correo phishing para acceder al link es una actualización, registrando el dominio reactivacion.es, el phisher puede usar una dirección como http://nombredelbanco.reactivacion.es, que pueda dar muy pocos motivos de sospecha a un usuario no experimentado.

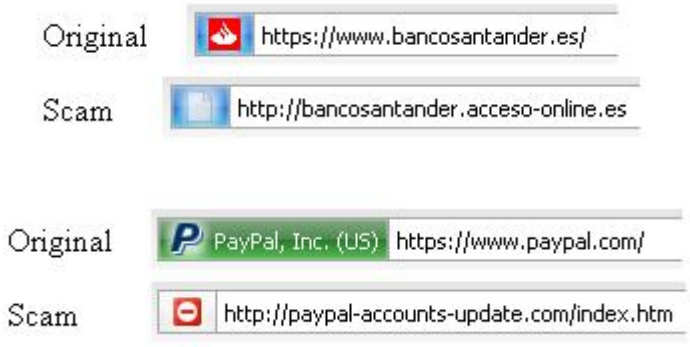


Figura 12. Modificación de dominios

- **Uso directo de dirección IP:** en vez de mostrar el nombre del dominio asociado al servidor de la página web fraudulenta, se puede usar directamente la IP y a continuación el nombre de la entidad bancaria de la siguiente forma: http://(ip servidor):80/nombredelbanco . La víctima puede pasar por alto los números que representan la dirección IP, ya que está acostumbrada a fijarse

unicamente en direcciones con letras. De esta forma sigue apareciendo el nombre de la entidad bancaria en la URL, que es lo que le da seguridad a la persona engañada.

Figura 13. Uso directo dirección IP

- **URL *Spoofing*:** es posible abrir una nueva ventana desactivando la barra de direcciones. De esta forma el usuario no tiene una URL de la que sospechar. Una vez desactivada la barra, también se puede optar por generar una barra falsa por medio de javascript. Estas técnicas también pueden introducir el icono de página web segura, incluyendo el certificado al hacer doble clic sobre este.

2.5.5 Nuevas modalidades de phishing

Poco a poco los delitos electrónicos van abriéndose camino en distintas tecnologías para poder llegar a más usuarios y de nuevas formas. Algunas de las modalidades que están apareciendo son las siguientes:

2.5.5.1 Smishing

Es una modalidad de phishing brasileño que usa mensajes cortos de teléfonía móvil (SMS). Esta técnica comenzó en Europa y Japón en el año 2006 y desde entonces ha ido extendiéndose por el resto del mundo poco a poco. El funcionamiento es similar, se le indica al usuario por medio de un SMS que ha sido suscrito a un determinado servicio y que éste le será cobrado a no ser que lo cancele a través de un enlace que se les proporciona en el mensaje, en el que se le piden sus datos personales. También se puede aprovechar el acceso del atacado a esa dirección para obligarle a descargar un troyano y poder usar los recursos de la escuela rusa.

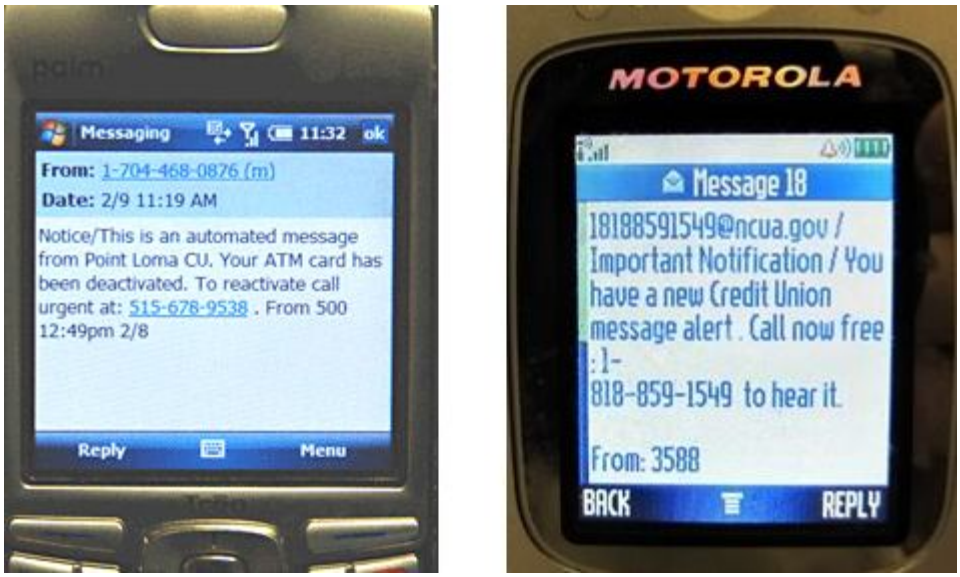


Figura 14. Ejemplos smishing

Hay una variante de smishing que consiste en la introducción de malware en un terminal móvil que se ocupa de recopilar todos los contactos contenidos en su memoria y enviarles uno a uno el mensaje.

La evolución de los teléfonos móviles hacia dispositivos más parecidos a ordenadores personales hace que sus sistemas operativos sean más vulnerables y que estén cada día más expuestos a ataques de este tipo. Estos sistemas son accesibles por múltiples vías:

- SMS - MMS
- Bluetooth - infrarrojos
- Páginas web
- Correo electrónico
- Conexión física a ordenadores

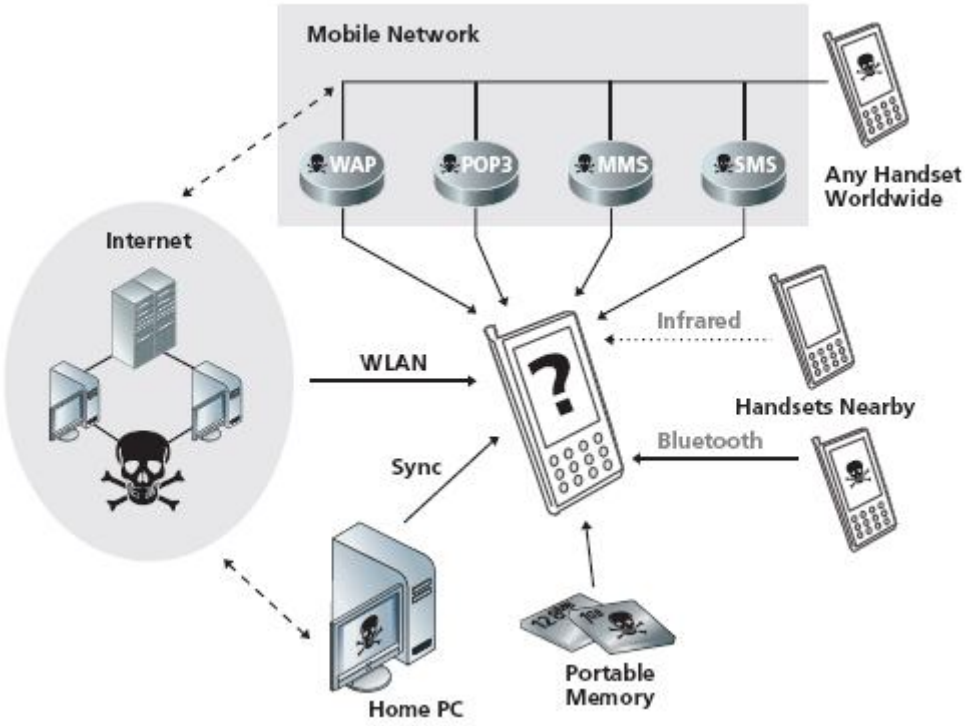
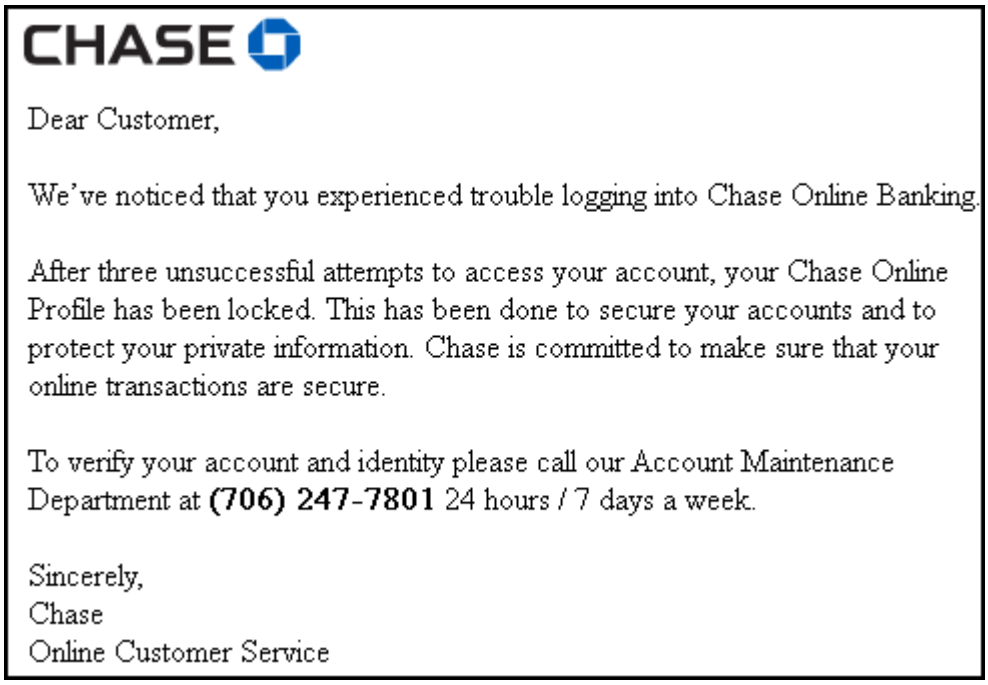


Figura 15. Vulnerabilidades telefonía móvil

Uniendo a esta diversidad de vías de acceso que los sistemas operativos de estos equipos están menos evolucionados y probados que los pertenecientes al mundo de los ordenadores y que el número de equipos es inmenso (más de mil millones en el año 2006 [20]), los terminales móviles son un objetivo cada vez más usado en la delincuencia electrónica [21].

2.5.5.2 Vishing

Es un fraude por medio de voz por IP. El usuario suele recibir un mensaje de correo electrónico en el que se le insta a que se ponga en contacto con una empresa determinada por medio de un teléfono que le es proporcionado. Una vez ha llamado, se le atiende usando alocuciones y música similar a la que usa la empresa real y una vez ganada la confianza, se le solicitan sus datos personales. El procedimiento es exactamente igual que el tradicional de la escuela brasileña, cambiando la página web falsa por un número de teléfono. Esta técnica puede resultar más eficaz que la común, ya que la sociedad tiene menos miedo al uso de medios de toda la vida como puede ser la teléfonía, antes que los medios electrónicos.


CHASE

Dear Customer,

We've noticed that you experienced trouble logging into Chase Online Banking.

After three unsuccessful attempts to access your account, your Chase Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Chase is committed to make sure that your online transactions are secure.

To verify your account and identity please call our Account Maintenance Department at **(706) 247-7801** 24 hours / 7 days a week.

Sincerely,
Chase
Online Customer Service

Figura 16. Ejemplo de correo vishing

También la primera forma de contacto con el usuario puede hacerse vía telefónica en vez de correo electrónico. Un marcador automático se encarga de realizar llamadas a una determinada zona y una vez descolgado el teléfono, reproduce una grabación que advierte sobre un problema con una tarjeta o sobre la congelación de una cuenta bancaria y un número de teléfono al que llamar para resolverlo. Esta forma puede ser muy eficiente en comparación con el correo electrónico no deseado, ya que el teléfono es un medio mucho más confiable.

Existen variaciones tipo man-in-the-middle, en las que el atacante consigue que el atacado llame a su número de teléfono y automáticamente enlaza la llamada con la entidad verdadera, quedando éste a la escucha de todos los datos que el atacado da a la empresa para proceder a su identificación.

En otras ocasiones redirigen al atacado al servicio de atención al cliente de la empresa verdadera sin necesidad de quedar a la escucha, ya que previamente se han encargado de preguntarle todos sus datos personales. La víctima no será consciente de este robo ya que ha seguido el procedimiento rutinario a la hora de contactar con el servicio de atención al cliente de la empresa: llamar, identificarse con todos los datos personales que le piden y pasar a hablar con un agente.

La voz sobre IP es una herramienta muy útil, ya que con muy pocos medios tecnológicos y económicos, se puede acceder al teléfono de millones de usuarios con toda comodidad. Existen programas gratuitos para crear centralitas virtuales que reciben llamadas de la misma forma que lo hacen las empresas y con voces grabadas similares a las centralitas de las entidades legítimas.

Gracias al mayor grado de confiaza que ofrecen este medio (junto a los sms del smishing) y a que estos conceptos apenas han calado en la sociedad en comparación con

los correos *spam* y el *phishing* tradicional, tanto *smishing* como *vishing* son técnicas muy eficientes en la actualidad a la hora de robar datos personales.

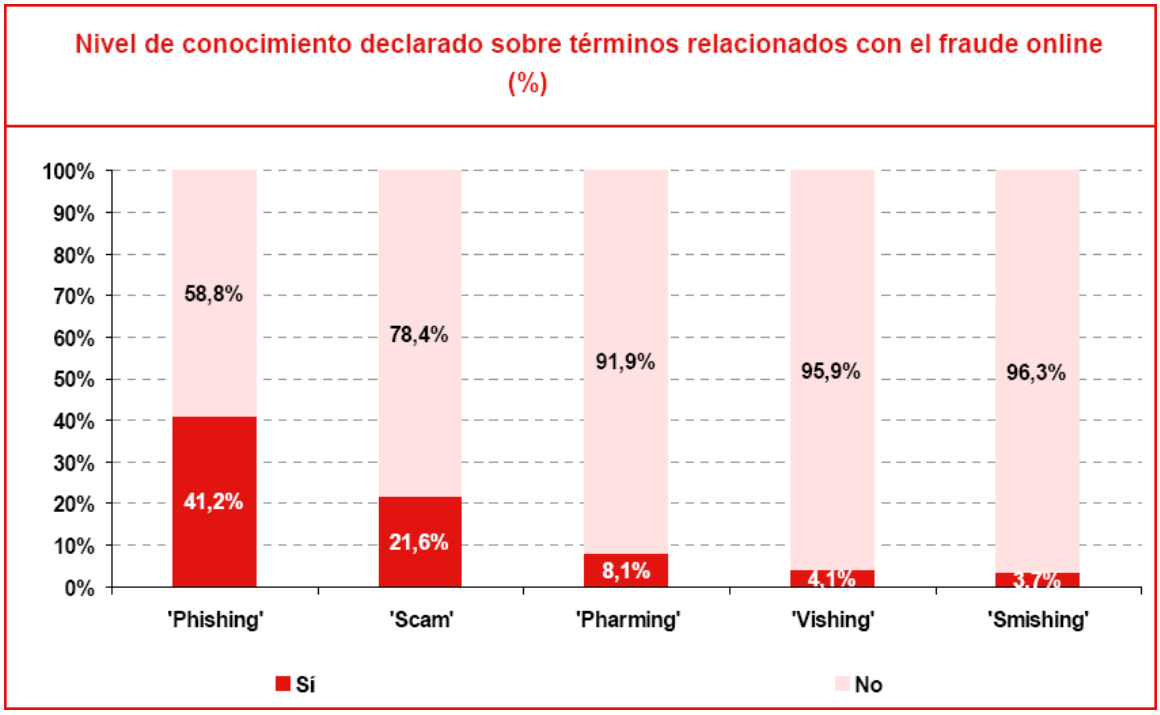


Figura 17. Grado conocimiento de técnicas de fraude bancario (Fuente: Inteco) [22]

2.6 Escuela rusa

2.6.1 Introducción

La escuela brasileña ha sido muy eficiente desde que comenzó a delinquir. No obstante, a lo largo de los años, los ususarios han ido concienciándose del peligro que puede presentar el hecho de atender a mails no solicitados o enlaces no confiables.

A pesar de que la escuela brasileña sigue consiguiendo objetivos, la escuela rusa poco a poco va calando en el mundo de la delincuencia electrónica. Sus medios permiten conseguir credenciales bancarias muchas veces sin necesidad de la ayuda del atacado y siempre sin la necesidad del uso de la ingeniería social.

Desde el punto de vista técnico, la escuela rusa es bastante más complicada que la brasileña y tiene un márgen mucho más amplio de evolución. Una de las características de la escuela brasileña es que sus herramientas son muy fácilmente detectables y son bloqueadas en cuestión de horas o días.

En la segunda parte del proyecto se estudiarán detalladamente múltiples ejemplos reales de estas herramientas.

2.6.2 Uso de malware

La escuela rusa hace uso de malware para infectar equipos y conseguir las credenciales que buscan. La infección de los equipos puede hacerse a través de puertas traseras, uso de vulnerabilidades de los sistemas o por medio del usuario, adjuntándolo en mensajes de correo electrónico, al estilo de la escuela brasileña. Los fines de la infección de equipos son muy variados:

- Abrir una puerta trasera para la posterior introducción de malware más avanzado.
- Obtener direcciones de correo con el fin de usarlas para el bombardeo de correos electrónicos.
- Buscar información personal como pueden ser nombres de usuario, contraseñas, páginas web visitadas, etc.
- Ataques *pharming*.

El uso de malware pasa desapercibido y puede recopilar datos sin generar sospecha alguna al usuario.

2.6.3 Pharming

Es un fraude que hace que el atacado no tenga ningún indicio para sospechar que se encuentra dentro de la red del atacante. Consiste en la modificación del sistema de resolución de nombres de dominio (*DNS*), haciendo que cada vez que el usuario intente acceder a su entidad bancaria, el navegador le dirija automáticamente a una página web *Scam*.

Este sistema es muy peligroso, ya que si el usuario no es consciente de que su ordenador ha sido infectado por un troyano, puede estar utilizando páginas web de *phishing* usando los accesos directos favoritos que siempre ha usado en su navegador, e incluso tecleando en la barra de direcciones directamente la *URL* original de su banco.

2.6.4 Keyloggers

Existen herramientas muy sencillas para captar las pulsaciones de teclado que se producen en un equipo. Su utilidad no es muy importante ya que desde hace tiempo, el sistema de validación de los portales bancarios se suele hacer a base de clics y no de introducción de datos por teclado.

No obstante, siguen siendo una herramienta útil para ciertos casos, en los que todavía no se utilizan teclados virtuales o siguen permitiendo la introducción de datos de forma corriente.

2.6.5 Programas espía

Existen evoluciones de *keyloggers* que contienen mayores y mejoradas funcionalidades, como pueden ser captación de clics e incluso envío de imágenes o videos de lo que aparece en el monitor del atacado. Con las versiones más recientes de estos programas, es relativamente sencillo obtener los mismos datos que se obtendrían estando sentado junto al atacado en persona.

El abanico de posibilidades que presentan este tipo de programas es muy amplio. Hay algunos que presentan decenas de funcionalidades y permiten monitorizar un equipo con todo detalle: procesos, eventos, ejecución de archivos, explorador de archivos, captura de pulsaciones, captura de imágenes, etc.

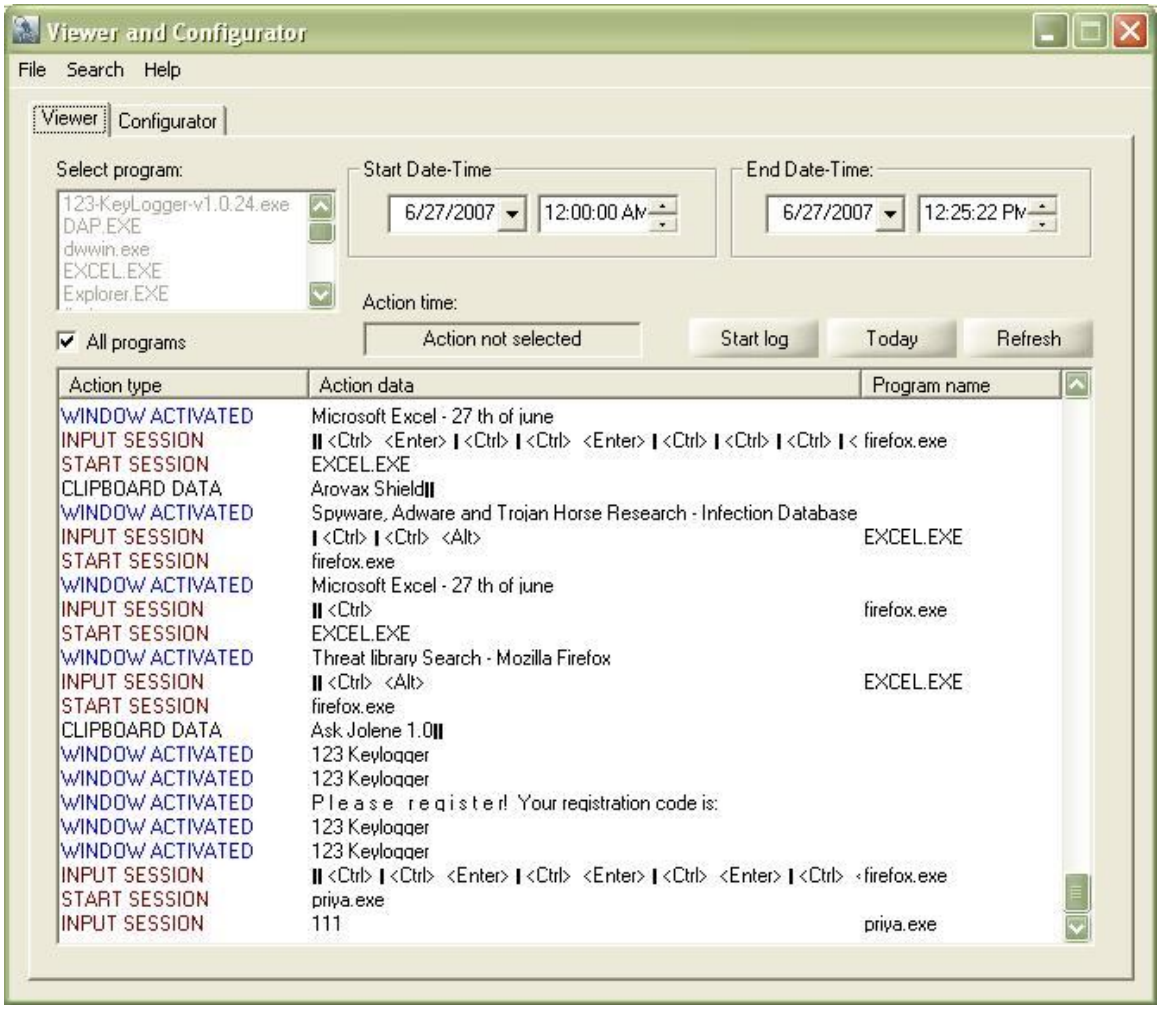


Figura 18. Ejemplo de programa espía

2.7 Robo de dinero

2.7.1 Introducción

El fin de la obtención de credenciales por los múltiples métodos comentados anteriormente es el acceso a cuentas y tarjetas bancarias para realizar compras o hacerse con dinero directamente.

Cualquier transacción electrónica es monitorizada por los bancos y todos los datos son guardados, de forma que sería muy sencillo encontrar al ladrón una vez ha accedido de forma ilegal a una cuenta ajena y ha realizado transferencias bancarias.

La forma de evitar que el delincuente sea interceptado por los servicios policiales es conseguir un intermediario que haga el trabajo por él y que sea la cabeza de turco. Estos intermediarios son conocidos como *mulas*.

2.7.2 Captación de mulas

Se utiliza el método por excelencia de la escuela brasileña, la ingeniería social. La forma de contacto principal vuelve a ser el correo electrónico. La víctima recibe normalmente una oferta de trabajo aparentemente real de una compañía importante, que consiste en un puesto de *gerente financiero*.

Lo único que se le pide es recibir dinero en su cuenta personal y reenviarlo a lo que supuestamente son clientes de la empresa. Se le ofrecen interesantes porcentajes de las transacciones.

Si la víctima acepta la oferta, normalmente se le enviarán un conjunto de documentos con apariencia oficial y se le pedirá que los firme para que todo parezca legítimo.

2.7.3 Uso de mulas

El delincuente usando los datos que previamente ha robado, realiza transferencias bancarias a la cuenta de la mula y le da la orden a esta de a dónde y cómo tiene que enviar ese dinero una vez descontada su comisión.

El reenvío de dinero se hace por medio de giros postales, como puede ser *MoneyGram*, *E-Gold* o *Wertern Union*. De esta forma es casi imposible rastrear el camino hasta el destinatario final.

Al cabo de pocos días, una vez la persona robada se ha dado cuenta de que ha desaparecido dinero de su cuenta y lo consulta con su entidad, el banco se pone en contacto con la mula preguntándole por qué ha recibido ese dinero en su cuenta, y

muchas veces responsabilizándole del robo, momento en el cual la mula se da cuenta de que ha sido víctima de una estafa.

Normalmente las mulas al principio no son conscientes de que están siendo partícipes de un delito.

El ciberdelincuente puede usar varias mulas a la vez, recibiendo en total una gran cantidad de dinero y a la vez dispersando las pruebas del delito. El hecho de recibir varias transacciones de cuantía moderada en comparación con una grande, ya sea desde una o varias cuentas robadas, limita la posibilidad de que el banco identifique la transacción como sospechosa y hace que la alarma se retrase. También baja el riesgo de pérdida para el delincuente en el caso de que una mula sepa realmente lo que está haciendo y desaparezca con el dinero.

Capítulo 3

Análisis teórico-experimental de delitos electrónicos

3.1 Introducción

Como se ha presentado en el capítulo sobre el estado del arte, para la realización de delitos electrónicos se precisan de muy diversas herramientas en cada una de las múltiples fases que requieren estos para el cumplimiento de sus objetivos.

En este capítulo vamos a estudiar detalladamente una gran variedad de herramientas reales utilizadas en la actualidad por los delincuentes del fraude bancario electrónico.

3.2 Captación de direcciones de correo

3.2.1 Introducción

Se ha realizado un estudio detallado sobre la recepción de correo spam. Como ya se ha comentado anteriormente, una dirección de correo es susceptible de ser conocida por diferentes vías:

- Rastreo web
- Mensajes en cadena
- Uso de malware
- Generación aleatoria de direcciones de correo
- Rastreamiento de grupos de noticias y listas de correo
- Formularios web fraudulentos

Como se ha estudiado anteriormente, en la escuela brasileña el primer paso a seguir es el contacto directo con la potencial víctima. Para ello es necesario tener una base de datos con direcciones de correo electrónico válidas.

3.2.2 Rastreo web

Existen multitud de programas encargados de conseguir direcciones de correo escaneando páginas web, ya sea de forma aleatoria, o recibiendo unos parámetros iniciales por parte del usuario. Aunque esta sea la forma principal, también suelen permitir encontrar direcciones en archivos variados. También permiten administrar estas direcciones ordenándolas, filtrándolas y exportándolas a otro tipo de ficheros.

A continuación presentaremos algunos ejemplos de este tipo de programas:

3.2.2.1 Super Email Spider

Este programa utiliza motores de búsqueda tales como Google, Lycos, iWon, Excite, Hotbot o MSN. Su funcionamiento es muy sencillo, se escribe una palabra clave, que es introducida en cada uno de los buscadores, y después recopila todas las direcciones de correo que aparecen en los resultados de búsqueda y en los enlaces que aparecen en éstos.

Permite configurar parámetros tales como la profundidad de búsqueda de enlaces o el número máximo de resultados y filtrar usuarios de direcciones comunes, como *subscribe*, *webmaster*, *root*, *admin*, *spam*, etc.

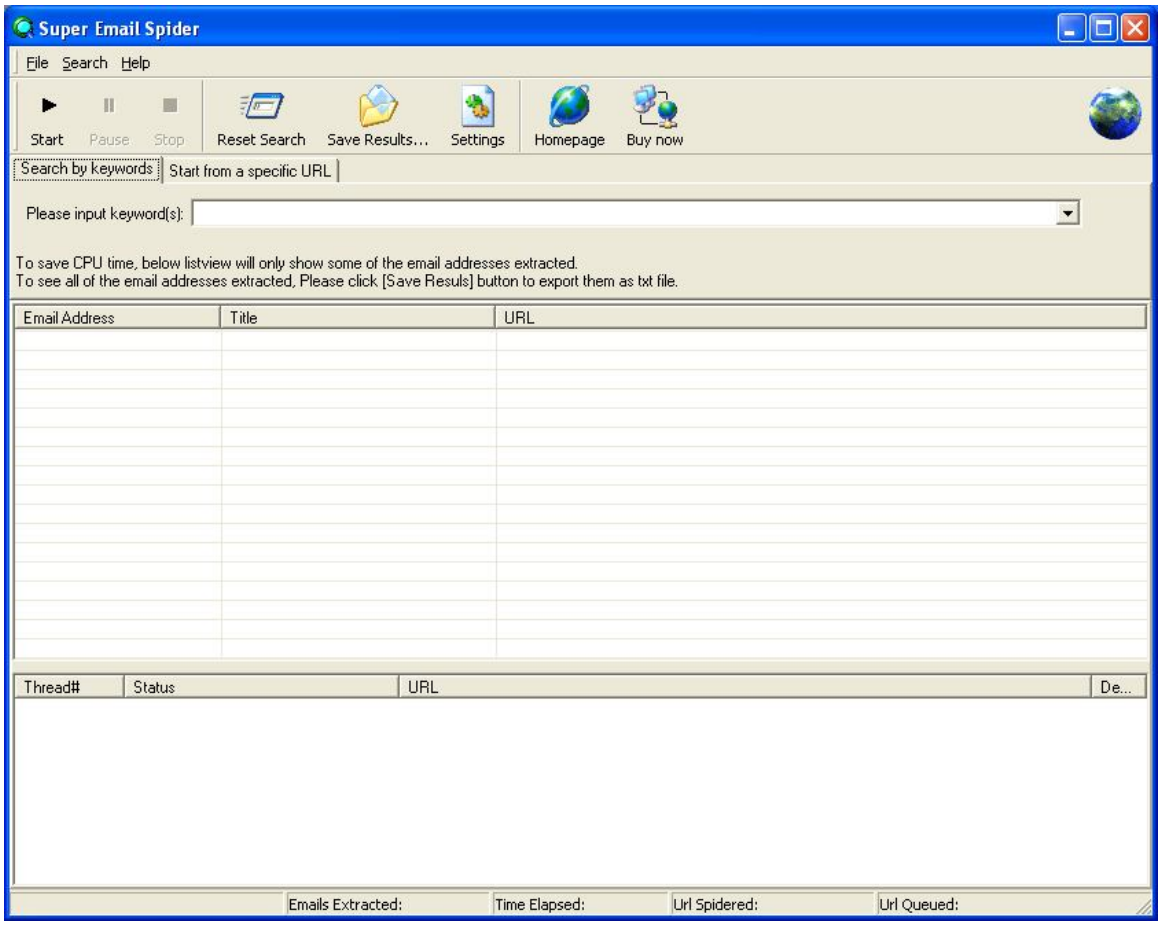


Figura 19. Super Email Spider. Pantalla principal

Para comprobar su eficacia, se ha realizado una prueba, usando los motores de búsqueda predeterminados por el programa, una profundidad de búsqueda de 2 y la palabra clave “correo”. Los resultados son:

- Direcciones de correo encontradas: 1516
- Tiempo empleado: 24 minutos
- URLs procesadas: 9362
- Rendimiento (direcciones por segundo): 1,05

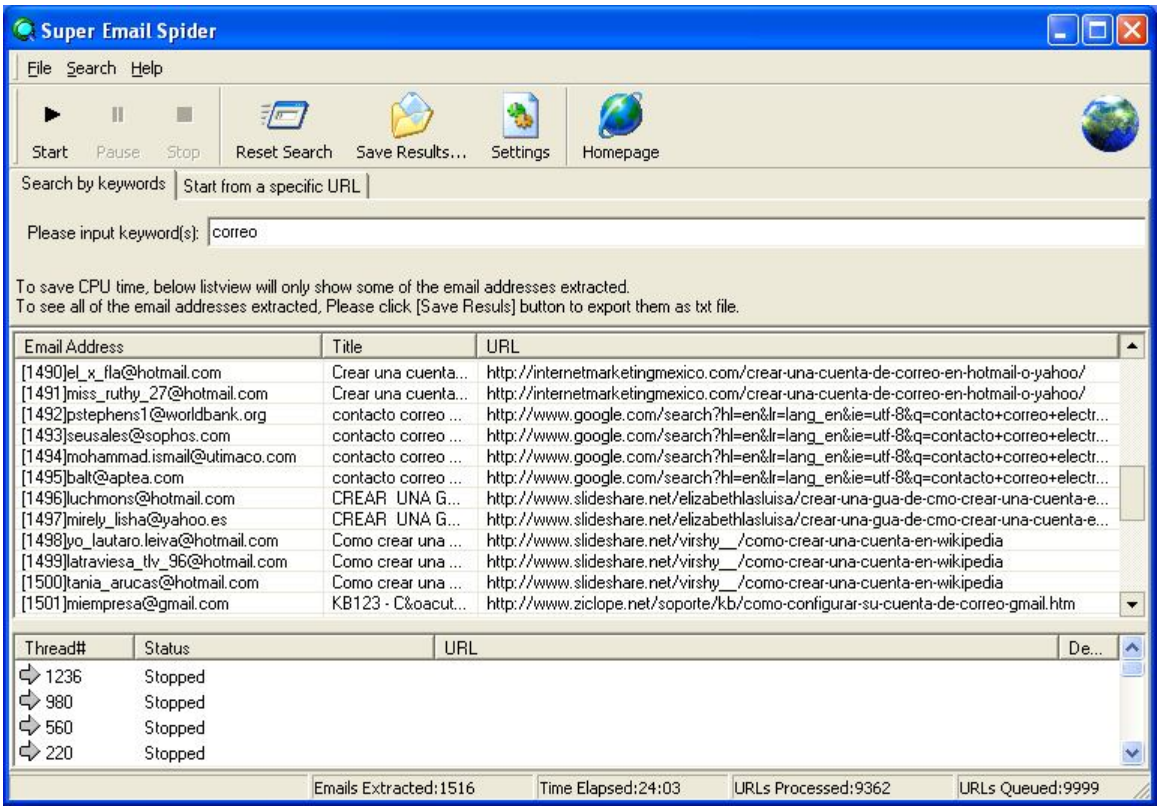


Figura 20. Super Email Spider. Resultado ejecución

Los resultados se guardan en un archivo *txt*

Figura 21. Super Email Spider. Direcciones captadas

3.2.2.2 Email Leecher

Este programa no se comercializa y es mucho más rudimentario. Sin embargo, su funcionamiento es muy eficiente.

Figura 22. Email Leecher. Pantalla principal

Simplemente hay que introducir el dominio de correo del que se quieren encontrar direcciones, el nombre de archivo en el que guardarlas y la cantidad de direcciones que queremos encontrar.

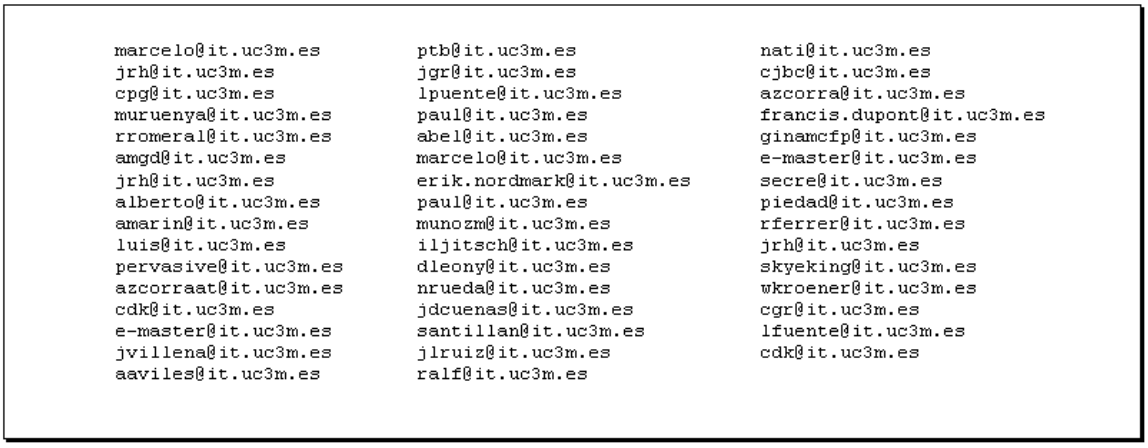
Para conocer el procedimiento que sigue para encontrar direcciones, se ha usado el analizador de redes *Wireshark*. Las capturas de tramas nos muestran que este programa solo utiliza el motor de búsqueda search.msn.com para obtener los resultados.

Se han realizado las siguientes pruebas:

- Probando con el dominio @it.uc3m.es, es capaz de encontrar 50 direcciones en menos de 10 segundos (>5 direcciones/segundo)
- Probando con el dominio @hotmail.com, encuentra 50 direcciones en 10 segundos (5 direcciones/segundo)
- Probando con el dominio @hotmail.com, encuentra 500 direcciones en 140 segundos (3,6 direcciones/segundo)

Figura 23. Email Leecher. Resultado

Tras varias simulaciones se puede concluir que la velocidad de búsqueda de direcciones es independiente del dominio y que a medida que se aumenta el número de direcciones deseadas, el rendimiento decrece.



```
marcelo@it.uc3m.es          ptb@it.uc3m.es              nati@it.uc3m.es
jrh@it.uc3m.es              jgr@it.uc3m.es              cjbc@it.uc3m.es
cpg@it.uc3m.es              lpuente@it.uc3m.es          azcorra@it.uc3m.es
muruenya@it.uc3m.es         paul@it.uc3m.es             francis.dupont@it.uc3m.es
rromeral@it.uc3m.es         abel@it.uc3m.es             ginamcfp@it.uc3m.es
amgd@it.uc3m.es             marcelo@it.uc3m.es          e-master@it.uc3m.es
jrh@it.uc3m.es              erik.nordmark@it.uc3m.es    secre@it.uc3m.es
alberto@it.uc3m.es          paul@it.uc3m.es             piedad@it.uc3m.es
amarin@it.uc3m.es           munozm@it.uc3m.es           rferrer@it.uc3m.es
luis@it.uc3m.es             iljitsch@it.uc3m.es         jrh@it.uc3m.es
pervasive@it.uc3m.es        dleony@it.uc3m.es           skyeking@it.uc3m.es
azcorraat@it.uc3m.es        nrueda@it.uc3m.es           wkroener@it.uc3m.es
cdk@it.uc3m.es              jdcuenas@it.uc3m.es         cgr@it.uc3m.es
e-master@it.uc3m.es         santillan@it.uc3m.es        lfuente@it.uc3m.es
jvillena@it.uc3m.es         jlruiz@it.uc3m.es           cdk@it.uc3m.es
aaviles@it.uc3m.es          ralf@it.uc3m.es
```

Figura 24. Email Leecher. Archivo txt con direcciones encontradas

3.2.3 Estudio sobre rastreo web

Hemos realizado un estudio para obtener una idea aproximada de cómo se proveen los atacantes de direcciones de correo por medio de rastreo web.

Para ello hemos creado las siguientes cuentas de correo:

- Dos de proveedores comunes: *Hotmail* y *Gmail*
- Dos con un proveedor propio: *phipro.blogsite.org*.

Para el proveedor propio hemos instalado un servidor de correo (*Argosoft Mail Server*) que permite ver todas las conexiones y diálogos SMTP que se establecen.

A lo largo de dos semanas, se fueron dispersando de la misma forma estas direcciones por multitud de foros españoles, a la espera de ser captadas y usadas para envío de correo no deseado.

Una vez realizada la diseminación de direcciones por la red, se procedió a activar el servidor de correo para realizar un estudio sobre captación y uso de direcciones para correo no deseado a lo largo de 9 meses.

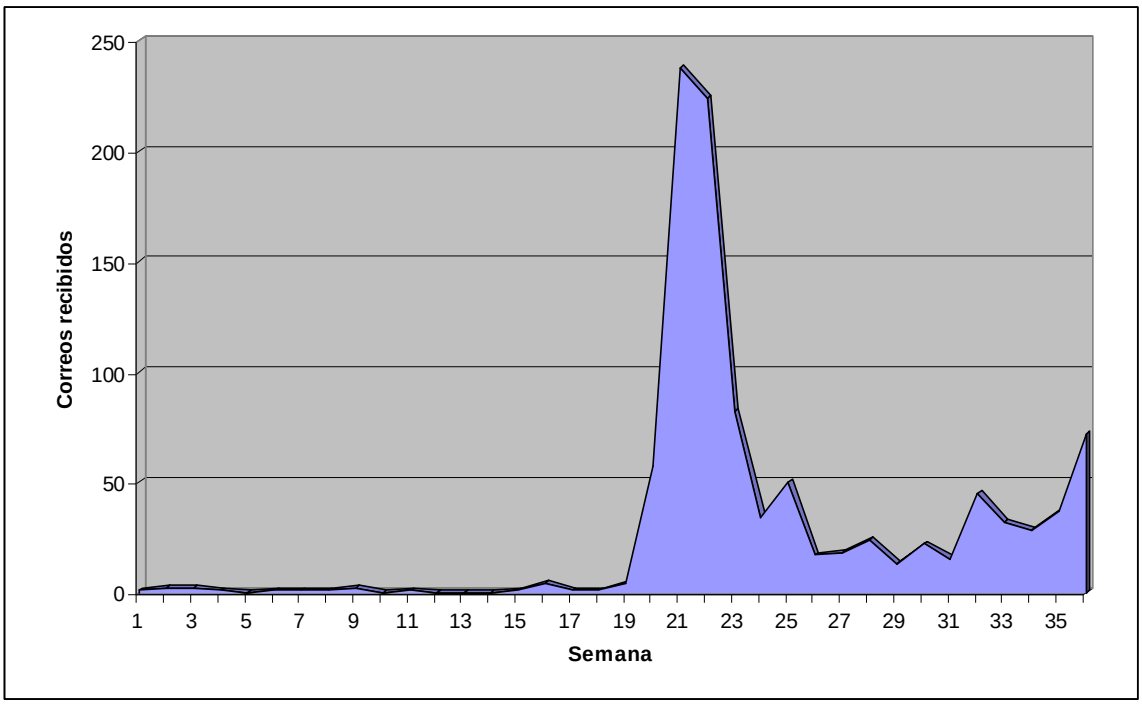


Figura 25. Recepción de spam a lo largo de 9 meses

Como se puede comprobar en el gráfico, hasta el cuarto mes no se comenzaron a recibir apenas correos. En el quinto mes hubo un gran ataque, probablemente la mayor parte de ellos desde el mismo sitio, y a partir de ahí, fue oscilando aunque se puede ver una línea ascendente en promedio.

Los miles de correos recibidos a lo largo de esos 9 meses fueron catalogados teniendo en cuenta su objetivo. El resultado es el siguiente:

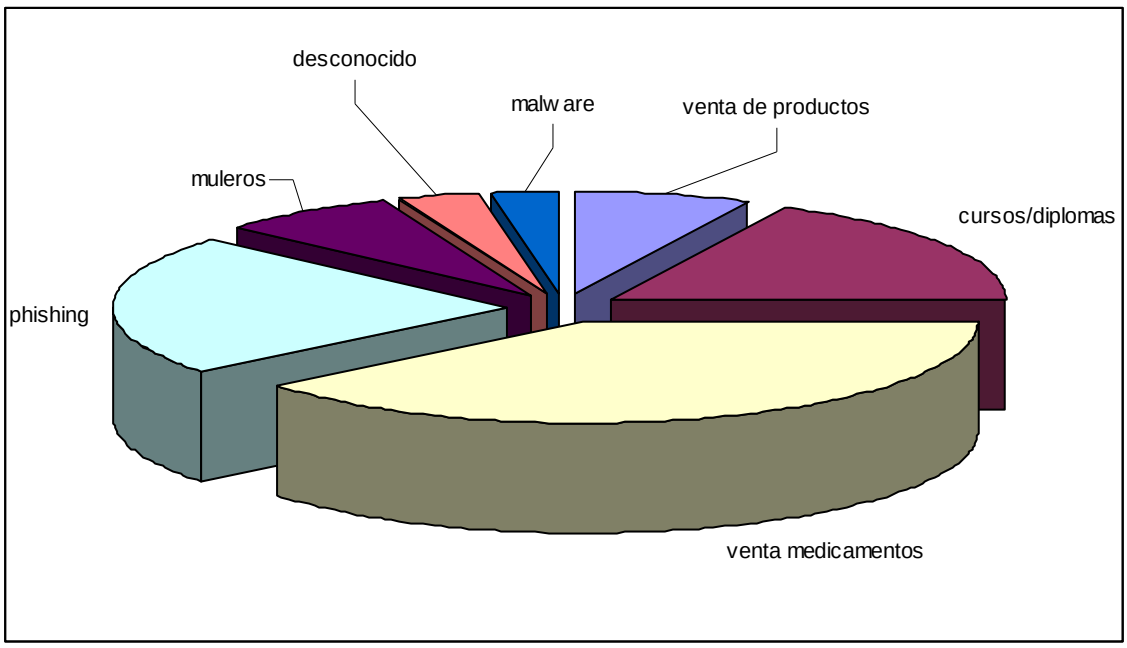


Figura 26. Objetivo de correos spam recibidos

Los resultados en cuanto a cantidad y tipos de correo recibido para las distintas cuentas han sido similares.

3.2.4 Conclusiones

Al cabo de unos meses, el correo no deseado recibido por las direcciones creadas era bastante menor que el que se recibe normalmente en una cuenta de correo de uso personal media. Esta observación nos permite deducir que la principal fuente de direcciones de correo válidas para los *spammers* es a partir de la captación de cadenas de mensajes y de malware espía.

Por lo tanto, se puede concluir que el verdadero peligro para el conocimiento no deseado de una dirección de correo es ajeno a su dueño, puesto que éste no puede controlar el uso que hace de ella una tercera persona a la hora de mandarla en el campo de un correo o de ser infectado por malware y extraída la libretas de direcciones.

No obstante, el hecho de tener una dirección de correo dispersada por páginas web, supone que a largo plazo sea captada por cada vez más robots buscadores de direcciones y hará que sea añadida a múltiples bases de datos de spam.

3.3 Correos phishing

3.3.1 Introducción

Vamos a analizar casos reales de correos electrónicos de la escuela brasileña. Estos correos han sido recopilados desde multitud de direcciones que se han ido obteniendo a lo largo de los meses que ha durado la investigación. Estas direcciones de destino han sido tanto personales como de cuentas “anzuelo” creadas para captar todo el spam posible (ver apartado anterior, *rastreo web*).

A continuación se mostrará una selección de los correos más característicos, presentando el contenido del correo, un comentario explicativo y marcado con números rojos de algunas particularidades. Solamente se va a atender a las características de estos mails, dejando para el siguiente apartado el contenido y ubicación de los enlaces que pretenden ser accedidos por el usuario.

3.3.2 Banesto

From: support12@banesto.es **1**
To: gutenberg@telefonica.net
Date: Fri, 24 Apr 2008 15:00:30 +0200 (added by postmaster@telefonica.net)
Subject: Nueva informacion de seguridad.
Hola, apreciado cliente:

Nuestro departamento de antifraude descubrió que la cantidad en su cuenta excede de dos mil euros. Para prevenir cualquier tentativa de una tercera persona de tener acceso a su cuenta personal hemos desarrollado un sistema de seguridad único que nos permite eliminar cualquier posibilidad de un acceso no autorizado.

El corazón de este nuevo sistema de seguridad es una autorización de cada transacción hecha de su cuenta personal. La autorización será aceptada después de que usted introduzca su numero pin de su tarjeta personal de seguridadl **2**:
- El número de seguridad contiene 6 dígitos
- La tarjeta personal de seguridad contiene una lista de 300 números pin
que pueden ser usados para la confirmación de sus transacciones.

En el caso que el número pin de su tarjeta personal de seguridad sea introducido tres veces incorrectamente, su cuenta será automáticamente suspendida. El número de seguridad sólo puede ser usado una vez para cada transaccion y es invalidado después de que la transacción es realizada.

Para solicitar el sistema de protección en Línea usted tiene que hacer clic en el link de abajo y seguir las instrucciones en pantalla. Si no tenemos noticias de usted dentro de 14 días su cuenta será bloqueada y tendra que ir a su oficina para que se la pongan de nuevo operativa.

En la última etapa de su registro asegurese **2** de introducir su direccion postal donde qquiere **2** que le enviemos su tarjeta personal de seguridad. Asegúrese que usted entra toda la informacion **2**correcta para evitar retrasos en recibir su tarjeta personal de seguridad.

La tarjeta la recibira **2** en un plazo de 14 dias por correo certificado después **2** de rellenar el formulario. Mientras tanto usted puede seguir usando su cuenta personal como hasta ahora.

Para ir al formulario presione aqui: Acceso a Banka por Internet **3**

Email ID: BNST8661qL
Atentamente.
Alfredo Camara Garcia.
Departamento de seguridad y asistencia al cliente.
Banesto (Banco Español de Credito).

Figura 27. Phishing Banesto

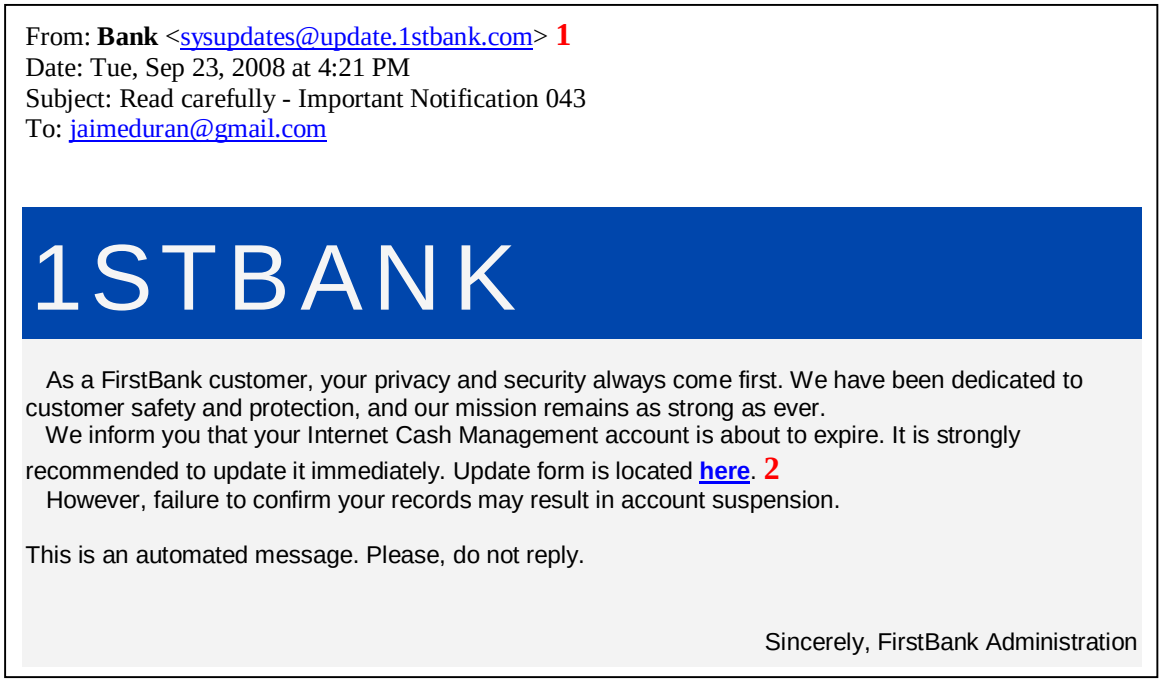
Este correo electrónico no pretende infundir miedo al destinatario. Anuncia una inocente actualización de seguridad con un link a una web falsa que recopila los datos personales de la víctima, pero sí que amenaza con bloquear la cuenta si no se procede a realizar los pasos requeridos en un plazo de dos semanas.

No posee ningún formato ni imagen, es simplemente texto.

1. **Campo from:** muestra una dirección del dominio original del banco. Por supuesto, no es real.

2. Faltas ortográficas
3. Acceso directo a *http://extranet.banesto-bank.com/*. Este dominio es un intento de parecer legítimo, aunque no tiene nada que ver con la entidad verdadera.

3.3.3 1st Bank


From: **Bank** <sysupdates@update.1stbank.com> **1**
Date: Tue, Sep 23, 2008 at 4:21 PM
Subject: Read carefully - Important Notification 043
To: jaimeduran@gmail.com

1STBANK

As a FirstBank customer, your privacy and security always come first. We have been dedicated to customer safety and protection, and our mission remains as strong as ever.
We inform you that your Internet Cash Management account is about to expire. It is strongly recommended to update it immediately. Update form is located **here**. **2**
However, failure to confirm your records may result in account suspension.

This is an automated message. Please, do not reply.

Sincerely, FirstBank Administration

Figura 28. Phishing 1st Bank

Este este caso, directamente se le dice al cliente que la cuenta está a punto de caducar y que tiene que actualizarla.

No posee ningún formato ni imagen, es simplemente texto.

1. **Campo from:** El dominio de la dirección de envío es un dominio falso y sin registrar.
2. Acceso directo a: *http://www.efirstbank.com.token-sk196dia21ued377ik26beg5242333mkn69axb60dw3khdu65gbs.s016.su/icm2/logonload.do*. El nombre del banco aparece en el dominio destino, pero realmente es un dominio diferente, con una larga cadena de caracteres aleatorios para despistar a la víctima.

3.3.4 Banco Colpatria

From: **Colpatria** <update@colpatria.com> **1**
Date: Tue, Sep 23, 2008 at 4:21 PM
Subject: Importante
To: spain@phipro.blogsite.org

Estimado cliente del **Banco COLPATRIA:**

Banco COLPATRIA hace todo lo posible por mantener al tanto al usuario de posibles problemas tanto en el servidor de **COLPATRIA** como en la cuenta del propio usuario. Por lo tanto, quiere advertirle en este momento que el departamento de seguridad cree que terceras personas an **2** podido haber accedido a su cuenta y han limitado esta para que no se produzcan operaciones no deseadas. Por lo tanto, el equipo del **COLPATRIA** le ruega que mediante el enlace que le proporcionamos confirme su cuenta inmediatamente para así poder fijar su ip como usuario principal y poder evitar más intromisiones en su cuenta:

Cuenta Personal:
http://67.162.218.175/ssh/colpatria/index.htm?nompag=comphtml/user.htm&tp=interno&id=8774W8YSfts296511YoDSgsd53Yxg52&usel=Activacion **3**

Cuneta **2** Empresarial:
http://67.162.218.175/ssh/colpatria/empresarial.htm?nompag=comphtml/user.htm&tp=interno&id=8774W8YSYM7296511ushSgsd53Yxg52&usel=Activacion **3**

COLPATRIA no se hace responsable de la perdida **2** de información en caso de que esta confirmación no se lleve a cabo.
Atentamente: **Banco COLPATRIA.**

Banco COLPATRIA

Figura 29. Phishing Colpatria

El destinatario es avisado de un acceso ilegal a la cuenta bancaria y su posterior bloqueo. Se le pide que acceda a uno de los enlaces proporcionados para confirmar la cuenta.

No posee ningún formato ni imagen, es simplemente texto.

1. **Campo from:** El dominio de la dirección de envío es el dominio verdadero del banco.
2. Falta ortográfica.
3. Accesos directos: directamente se pone la dirección IP del servidor destino, añadiendo a continuación el término ssh para hacer pensar que es un dominio seguro y también el nombre del banco.

3.3.5 Caja Madrid

---------- Forwarded message ----------
From: **Caja Madrid** <correo@cajamadrid.es> **1**
Date: 2008/10/15
Subject: Aviso Importante
To: "undisclosed-recipients:"@smtp.uc3m.es

CAJA MADRID **2**

Notificamos que su Servicio en lnea **3** se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en lnea.

Como medida de seguridad hemos decidido desactivar su cuenta temporalmente, este incidente puede deberse a que realizo intentos de acceso a su cuenta desde otra direccin IP debido a el **3** sistema dinmico **3** que utilizan los proveedores de Internet.

Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado :

PARTICULARES **4**

Aviso Importante : Le aconsejamos terminantemente realizar el servicio de activacin 3 haciendo clic en el enlace correspondiente en un plazo no mayor a 24 horas para no ser suspendido su servicio de banca en lnea 3.

---

oficina internet
CAJA MADRID

Caja de Ahorros y Monte de Piedad de Madrid, CAJA MADRID, C.I.F. G-28029007, Plaza de Celenque, 2. 28013 Madrid.
Registered on the Madrid Mercantile Register on page 20; volume 3067 General; sheet 52454; and with the Special Savings Bank Register under number 99. Cdigo B.E.: 2038. BIC Code: CAHMESMMXXX. Credit entity subject to supervision by the Bank of Spain

Figura 30. Phishing Caja Madrid

Aquí también se avisa de un bloqueo de la cuenta debido a varios intentos fallidos de acceso. Se pide acceder a un enlace para reactivar la cuenta.

1. **Campo from:** El dominio de la dirección de envío es el dominio verdadero del banco.
2. La imagen del emblema de la entidad se carga directamente de la página web oficial (*http://www.cajamadrid.es/Portal_Corporativo/imagenes/logo_home.gif*). Sin embargo, contiene un link a la página web falsa.
3. Faltas ortográfica abundantes. Las vocales que deben llevar tilde ni siquiera aparecen.

4. El enlace lleva a *http://058177149067.ctinets.com/b.html*, un dominio que nada tiene que ver con el original. No obstante, la imagen se descarga una vez más de la página oficial (*http://www.cajamadrid.es/Portal_Corporativo/imagenes/tag_particulares_on_an.gif*).

3.3.6 La Caixa

De: **la Caixa** <correo@orange.es> **1**
Fecha: 23 de octubre de 2008 4:13
Asunto: [bectalleraulacsj] [talleraulacsj] Usted tiene (1) Mensaje de "la Caixa"
Para: "undisclosed-recipients:"@smtp.uc3m.es

"la Caixa" **2**

Notificamos que su Servicio en lnea se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en lnea.

Como medida de seguridad hemos decidido desactivar su cuenta temporalmente, este incidente puede deberse a que realizo **3** intentos de acceso a su cuenta desde otra direccin IP debido a el **3** sistema dinmico que utilizan los proveedores de Internet.

Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado :

Click Aqui Para Acceder Linea Abierta **4**

Aviso Importante : Le aconsejamos terminantemente realizar el servicio de activacin 3 haciendo clic en el enlace correspondiente en un plazo no mayor a 24 horas para no ser suspendido su servicio de banca en lnea 3.

Caja de Ahorros y Pensiones de Barcelona, la Caixa, C.I.F. NIF G-5889999/8, PAv. Diagonal, 621-629 08028 Barcelona.
Registered on the Barcelona

Figura 31. Phishing La Caixa

Este caso es similar al anterior de Caja Madrid. Prueba de ello es que las incorreciones ortográficas son las mismas. Todo apunta a que está generado por el mismo grupo delictivo o al menos por el mismo software generador de phishing.

Se recibió minutos después en otra cuenta un correo idéntico pero con el nombre de Cajamar en vez de La Caixa.

1. **Campo from:** curiosamente el dominio remitente que muestran es *Orange*, empresa de telecomunicaciones que nada tiene que ver con la entidad bancaria que pretenden suplantar.
2. De nuevo, el emblema proviene directamente de la entidad verdadera (*http://portal.lacaixa.es/StaticFiles/StaticFiles/ddc8c97b5e4eb110VgnVCM1*

000000e8cf10aRCRD/es/logo_laCaixa_principal.gif), y el enlace que presenta es el mismo que el del punto 4.

3. Faltas ortográficas
4. Enlace a *http://corp-200-105-248-118-uio.punto.net.ec/icons/maria.html*, no presenta ninguna similitud con la entidad suplantada.

3.3.7 Banesto 2

De: **Banesto** <info@banesto.es> **1**
Fecha: 30 de octubre de 2008 14:03
Asunto: información importante
Para: "undisclosed-recipients:"@smtp.uc3m.es

Banesto **2**

Atención al Cliente

Banesto es la primera entidad financiera que ha obtenido el certificado AENOR de Calidad de Servicio y gestión de la satisfacción de clientes.

Nuestro objetivo es ofrecer el mejor servicio al cliente y por eso trabajamos para que sus opiniones nos ayuden a mejorar.

Por eso nosotros ya estamos introduciendo todo tipo de promoción por nuestros clientes. Te ofrecemos premios en valor de 500, 1000 euros cada uno!

Nunca nadie habia hecho nada parecido. Aprovecha la ocasión y no dejes escapar esta oportunidad.

¡Es muy fácil ganar premios!

ENTRAR >> **3**

Solo se acepta una partipación.
Solo los clientes de Banesto, estan acceptados como participantes.
Los ganadores van a estar contactado a traves de teléfono.

Figura 32. Phishing Banesto 2

En este correo no se ha utilizado ningún método para infundir miedo. El mensaje es positivo, planteando la obtención de un certificado de calidad por parte de la entidad y la participación en un sorteo por parte del cliente.

Este ha sido uno de los pocos correos phishing escrito correctamente.

Se recibieron en el mismo día correos idénticos con el logo y la dirección de envío de Caja Madrid y La Caixa, cambiando en la URL de acceso únicamente el nombre del banco.

1. **Campo from:** la dirección aparenta ser totalmente legítima.
2. El emblema proviene de la propia entidad (*http://www.banesto.es/NBanesto/img/loBanestoLazo.gif*).
3. El enlace de acceso es *http://banestoinfo.110mb.com/*. Nuevamente se usa el nombre de la entidad suplantada en parte de la URL.

3.3.8 Agencia Tributaria

De: Agencia Tributaria [mailto:impuestos@aeat.es] **1**
Enviado el: martes, 01 de septiembre de 2009 17:59
Para: undisclosed-recipients:
Asunto: Reembolso de Impuestos

Notificación de Impuestos

Agencia Tributaria

2

Después de los cálculos del último informe anual de su actividad fiscal hemos Determinado que usted es elegible para Recibir un reembolso de impuestos de 186.80 euros.

Por favor, envíe la solicitud de reembolso de impuestos y nos permiten 3 días para procesarla.

Para acceder al formulario para su reembolso de impuestos, haga clic aquí **3**

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación de los registros inválidos o aplicándose después del plazo.

Documento de Referencia: (92054568).

© Agencia Tributaria

Figura 33. Phishing Agencia Tributaria

En este caso la forma de convencer es ofreciendo un dinero rápido, haciendo creer a la víctima que puede recuperar dinero de sus impuestos.

Al igual que el anterior ejemplo, este correo está escrito de forma correcta, al contrario que la mayoría de los casos de *phishing*.

1. **Campo from:** la dirección aparenta ser totalmente legítima.
2. El emblema proviene de la propia entidad.

3. El enlace de acceso es *http://mail.oceanic-fruits.com/*. No tiene nada que ver con la entidad. La página estaba bloqueada en el momento de recepción del correo.

3.3.9 Todd Williams: caso de estafa directa

En este caso, en vez de suspuestamente contactar con la víctima una entidad, lo hace directamente un directivo. El objetivo es recibir directamente el dinero en una cuenta, sin necesidad de robar credenciales.

El correo es el siguiente:

De: HERRY LITTLE <little.189@osu.edu> **1**
responder a: <todd_williams_101@hotmail.com>**2**
para: **3**
fecha: 7 de diciembre de 2008 08:46
asunto: Dear Friend,

Dear Friend,
I am Todd Williams, I am a staff of Natwest Bank Plc,U.k.i have a very Urgent Business proposal of (£18,500,000.00 Million Pounds)for you to handle with me from my bank.And finally I shall provide you with more details of this transaction, , Please reply to my private box.
Mr. Andreas schranner **4**, property magnate who was based in the U.K., who happens to be one of our very good clients. On the 31st of July 2000, Mr. Andreas schranner **4**, his wife Maria , their daughter Andréa eich **4**, her husband Christian, and their children katharina **4** and maximilian **4** all died in the air **4** France concord **4** plane crash bound for New York in their plan for a world cruise.

This is the link,
http://news.bbc.co.uk/1/hi/world/europe/859479.stm

email:(todd_williams_101@hotmail.com)
Kind Regards,
Todd Williams(Mr.)
ACCOUNTS OFFICER

Figura 34. Correo Todd Williams

Observaciones:

1. **Dirección de envío**: una vez más, se utiliza el dominio de la Universidad de Ohio. Probablemente se haya utilizado en este correo la misma herramienta de envío de correo masivo y genere direcciones similares. Es bastante desconcertante que un trabajador de banco contacte con alguien por motivos de trabajo y utilice una dirección de este tipo.
2. **Dirección de respuesta**: se utiliza una dirección de servicio de correo gratuito para poder recibir respuestas.
3. El destinatario del correo aparece en blanco, lo que muestra el nulo nivel de personalización que presenta el correo.
4. Una vez más, los errores gramaticales saltan a la vista. Abundan la falta de uso de mayúsculas.

La estafa en este caso consiste en hacerse pasar como trabajador de un banco famoso y ofrecer un negocio que consiste en manejar una cantidad enorme de dinero. Para ello muestra la historia del que se supone es un gran cliente del banco, y que en el año 2000 murió junto con el resto su familia. De esta forma, se incita a la víctima a contestar para pedir más información, pues se da a entender que el negocio tiene algo que ver con dinero de seguros o herencias.

El enlace a la noticia es real y forma parte del archivo de las noticias de la *BBC*:

Figura 35. Enlace a noticia. Todd Williams

Unos días después de contestado el correo, se recibe otro, esta vez desde la cuenta a la que se envió la respuesta.

De: Todd Williams <todd_williams_101@hotmail.com>
Para: <pascasioking@gmail.com>
fecha: 14 de diciembre de 2008 19:44
Asunto: READ AND GET BACK TO ME !!
enviado por: hotmail.com

Good day,

Thank you for your mail and your willingness to help me, I am intrested in transfering the funds of one of our late customers to your account as All attempts to trace his next of kin were fruitless. My position here at my office requires me to investigate and I therefore made further investigations and discovered that Mr. Andreas Schranner did not declare any next of kin or relation in all his official documents, including his bank deposit paperwork in my bank.According to the British Law. The money will revert to the ownership of the British government if nobody applies to claim the fund. To avoid this money being sent to the British treasury as unclaimed funds, I have decided to seek your assistance to have you stand as his next of kin so that the said fund (£ 18,500,000.00 Million Pounds), would be released in your name as the next of kin and paid into your account.All documents and proof that will have you claim this fund will be forwarded to you without any stress upon your response to this mail more soon, I want to inform you that I have unanimously agreed to offer you (£4m) of the total sum for the assistance and role you are going to play in this transaction,(£2m)will be given to charity organizations in your country with your supervision while the remaining will be for me.
You have to follow the normal banking procedures before this funds can be released to your local bank account in your country, as i said you will take 40% from the total amount. The funds are in Pound sterling. So it is not a joke ,But i want you to be aware that i might not have the time to come over to your place as most of this transaction will be done online , Now i need to know more about you, what do you do for a living? if you can handle this funds?? I will also require your full legal name as the funds will be transferred through your name, so that the Lawyer can prepare the documents in your name .

Can i trust you? are you married with kids? I will also want you to send me your passport copy if you are serious and i will also send you my own OK, trust is very important for this transaction.

Please it is very important i know who i am dealing with. This business is hitch free so do not worry about getting into trouble, there is no risk involved at all. Everything can be concluded within four to six banking days , and the bank will have to release the funds to you, I have the file of the Client here with me, that we will use to support the claim.

We need to move fast. Once i get a positive response from you, i will send you the Application Release Letter and the bank's contact details, so that you can send the letter to them by email. So that they can release the funds to us. You can call me on : +447031960882 at anytime as it is my private mobile phone. I will wait for your call or call you any moment on your mobile line. Thank you but i need you to send an immediate response via email as i am at my desk awaiting your response. I have attach my identification for your perusal so that you will know who you are dealing with . I will appreciate if you do same .

Kind Regards ,
Todd Williams (Mr.)

Figura 36. Correo Todd Williams 2

Este correo fue acompañado de una imagen escaneada de la tarjeta de identificación de Todd Williams con el objeto de dar mayor credibilidad al asunto:

Figura 37. Tarjeta identificación. Todd Williams

El remitente nos termina de contar la historia que empezó a narrar en el primer correo. Dice que el fallecido no tiene más herederos declarados vivos y que de no hacer algo, los 18,5 millones de libras que posee serán entregados al gobierno británico. Ofrece que nos declaremos como pariente del fallecido para poder heredar la fortuna. El pacto consiste en que parte será para nosotros, parte se donará a la beneficiencia y el resto se lo quedará la persona que nos propone el trato.

En el siguiente correo, amplía la información:

De: Todd Williams <**todd_williams_1121@hotmail.com**>
Para: <pascasioking@gmail.com>
fecha: 18 de marzo de 2009 06:16
Asunto: MORE DETAILS OF THE TRANSACTION !!!
enviado por: hotmail.com

Dear Partner,

Thank you very much for response and your interest in this transaction, I am also glad to note that you are noble and trustworthy person whom I can rely on for your capabilities to handle this transaction. I have not contacted anybody but you for assistance , after reading your last email i became more convinced of your ability to see this through , i am now more sure of your willingness, trustworthiness and commitment to execute this transaction with me after reading your message, I cannot afford to compromise these virtues Considering the huge amount involved, it is necessary for me to be sure of the person to whom I will be entrusting this money to, Actually my trust is not given out lightly but something in my heart tells me i can trust you to deliver, I will send your full names to the local Attorney here in London who will represent prepare all the documents to ensure the funds are released to you without your physical presence here in the United Kingdom after i have been able to source out a reliable Lawyer later today .

READ THE FOLLOWING AND GET BACK TO ME:
Firstly,You should note that this project is highly capital intensive. This is why I have to be very careful. I need your total devotion and trust to see this through. I know we have not met before, but I am very confident that we will be able to establish the necessary trust that we need to execute this project within the next couple of days when the transfer to your local account in your Country will be completed .

Furthermore, to ensure our success i shall be responsible for paying the processing of the relevant affidavits and documents in your name to put you as the legal beneficiary of the funds and I will take care of the cost of retaining the services of the Attorney and to have the transfer documents perfected as soon as possible so that the release process can commence without any undue delays. He shall draft the necessary Affidavits which shall put you in place as next of kin after obtaining the Letter of probate/Administration and power of Attorney and he shall then be handling all matters of probate on your behalf as far as this transaction is concerned, I will handle these costs on my side.

To ensure that the funds are transferred to your local account in your own country, you will be required to open an offshore/online account with my bank from where you will personally transfer the funds to your local account from your own computer through our secured website. It is necessary for me to let you know that you will be required to take care the cost of opening the account and having the account activated as you will be dealing directly with NatWest Bank . You have to realize that although i am an insider, i will prefer you deal Directly with the concerned Bank official. The reason I am telling you this is because the Bank will not transfer the money from here to you without recommending that you open an online account with it and have it ready to transfer the funds, I do not want any complications.What I expect from you is trust , commitment and total co-operation , I want this money transferred with your assistance out of My bank If we act fast enough and you show enough commitment ,we could complete the project within a maximum of five banking days, hence we must remain on continuous correspondence daily by email, I will send you the application release letter so that you can send it to the bank at once .I shall be expecting a positive feedback and assurance from you as soon as possible, everything is ready on my side for the successful completion of this project, I earnestly await your response.

Sincerely,
Todd Williams (Mr.)

P:S Do not forget that details of this transaction remains CONFIDENTIAL as i do not want you to draw undue attentions to yourself as a result of this huge funds you are expecting in your bank account soon .

Figura 38. Correo Todd Williams 3

Se puede observar que la dirección de envío ha pasado de ser *todd_williams_101@hotmail.com* a *todd_williams_1121@hotmail.com*. Esto demuestra que el estafador se ha creado varias direcciones similares para dejar menos rastro o no verse limitado si el proveedor le bloquea alguna cuenta por haber recibido alguna denuncia.

En este tercer correo el remitente resalta la confianza que tiene en nosotros, a pesar de que en las respuestas sólo se le ha solicitado más información, sin realizar ningún comentario personal.

También comenta los pasos que hay que seguir. Queda claro que hay que abrir una cuenta electrónica si no la tenemos y que no hay que comentarlo con nadie, puesto que es muy importante que sea un asunto confidencial.

Una vez contestado, recibimos otro correo.

De: Todd Williams <todd_williams_1121@hotmail.com>
Para: <pascasioking@gmail.com>
fecha: 18 de marzo de 2009 10:27
Asunto: LEGAL ASPECTS OF THE TRANSACTION .
enviado por: hotmail.com

Dear Partner ,

Thanks for your response , this is exactly the kind of attitude that this transaction will require within the next couple of days ,I am proud to inform you that i have finally employed the services of a local Attorney who will perfect the legal aspects of this transfer and will also act in proxy on your behalf so that the Bank can release the funds to you within the next couple of days without your physical presence here in the United Kingdom ,I want you to note that you are going to be contacting the NatWest bank directly and deal with the bank independently but with my advice and close supervision , the offshore account that will facilitate the online transfer is going to be operated by you and you can keep the bank account information to yourself if that will make you feel safe , i want you to realize that i will be counting on you to disburse my share of the funds after you have received the money from the Bank .

I am relieved that everything is going according to plan ,I will send you the application release letter in my next email so that you can send it to the bank immediately .This is the first major step you are expected to take as the beneficiary . Once the Bank receives the application letter , they will begin the machinery to effect the transfer to you .

I will recommend that you restricts your correspondence to the bank to email messages for now so that you will not make any mistake as you will need to obtain advice from me before taking any major steps .The Lawyer has demanded that i pay £ 18,000 to enable him complete the paper work to put you in place as the legal beneficiary of the Inheritance and which i have done.Note as i have previously stated in my mail to you that you would be responsible for the activation of that account as this will be the only blocking stone to our success.I am ready to make any sacrifice to get this matter concluded asap and i hope you of this same mind . I do not want anything to stand between the successful completion of the transfer to your local account in the next few days .

Kind Regards ,
Todd Williams

Figura 39. Correo Todd Williams 4

Una vez más, resalta la confianza que tiene en nosotros y lo que le gusta nuestra actitud, sin haberle contestado más que una frase.

Este fue el último correo que se recibió. Al cabo de unos días, ambas cuentas de Hotmail estaban bloqueadas, por lo que es de esperar que el delito fue interceptado a tiempo. Este es el típico caso en el que una vez se ha ganado la confianza de la víctima y se la ha hecho creer que va a ganar una gran suma de dinero, se le pide una pequeña cantidad para algún gasto inesperado y una vez realizada la transferencia, el delincuente desaparece.

3.3.10 Conclusiones

Después de estudiar decenas de correos electrónicos fraudulentos y de haber presentado anteriormente varios ejemplos de los más característicos, se puede concluir:

Direcciones de envío

- Las direcciones desde donde se envían los correos son falsas o pertenecientes a otras personas. En la mayoría de los casos se procura que aparezca el nombre de la entidad suplantada para dar mayor credibilidad.
- Claramente estos correos no se envían desde cuentas normales, sino desde servidores de correo spam preparados para automatizar envío de correos modificando destinatarios que se obtienen de bases de datos y evitando repeticiones que puedan comprometer la credibilidad del contenido.

Contenido de los correos

- El contenido de los correos siempre tiene una intención de llamar la atención del destinatario, empujándole a acceder a un enlace lo más rápidamente posible.
- El 95% de los correos tiene faltas ortográficas. En la mitad de ellos su número e importancia hacen que estos sean automáticamente rechazados por el destinatario.
- Las incorrecciones ortográficas de un 25% de los correos son simples faltas de tildes, que pueden pasar perfectamente desapercibidas por muchos destinatarios.
- Aproximadamente la mitad de los correos son demasiado simples. No incluyen imágenes, ni el logo de la empresa. Estos correos son muy poco eficaces, puesto que hacen pensar que no provienen de la entidad verdadera.

Enlaces

- Los enlaces de acceso proporcionados a una *página web scam* normalmente incluyen el nombre de la entidad bancaria y palabras como *update, clientes, acceso, ssh, secure*, etc. El objetivo de esto es dar mayor credibilidad al enlace y que este sea accedido al eliminar posibles dudas por parte de la víctima.
- En muchas ocasiones, en el momento de la recepción de los correos, estos enlaces ya habían sido anulados. Las últimas versiones de los navegadores *Firefox* e *IExplorer*, son capaces de avisar al usuario sobre el peligro de muchos de estos enlaces antes de que estos hayan sido eliminados, gracias a programas de aviso de suplantación de identidad.
- El máximo tiempo que ha durado activo un enlace a una página scam es de 24 horas, lo demuestra la rapidez que se precisa para enviar correos y que estos enlaces sean accedidos.

3.4 Páginas web scam

3.4.1 Introducción

Como se ha comentado en el estado del arte, el objetivo de los correos phishing es simplemente el conseguir que el destinatario acceda a una página web fraudulenta, que normalmente es una copia de la original.

En este apartado vamos a ver las muestras más características que se han recolectado de páginas web scam, enlazadas en los correos phishing recibidos.

A continuación pasaremos a mostrar algunos ejemplos de este tipo de páginas, junto con sus mails correspondientes, que no serán comentados, pues ya se han caracterizado en el apartado anterior.

3.4.2 La Caixa

Correo electrónico recibido:

From: **la Caixa** <correo@orange.es>
Date: 2008/10/23
Subject: Usted tiene (1) Mensaje de "la Caixa"
To: "undisclosed-recipients:"@smtp.uc3m.es

Notificamos que su Servicio en lnea se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en lnea.

Como medida de seguridad hemos decidido desactivar su cuenta temporalmente , este incidente puede deberse a que realizo intentos de acceso a su cuenta desde otra direccin IP debido a el sistema dinmico que utilizan los proveedores de Internet.

Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado :

Click Aqui Para Acceder Linea Abierta

Aviso Importante : Le aconsejamos terminantemente realizar el servicio de activacin haciendo clic en el enlace correspondiente en un plazo no mayor a 24 horas para no ser suspendido su servicio de banca en lnea.

Caja de Ahorros y Pensiones de Barcelona, la Caixa, C.I.F. NIF G-5889999/8, PAv. Diagonal, 621-629 08028 Barcelona. Registered on the Barcelona

Todos los derechos reservados.

Figura 40. Correo Scam La Caixa

El enlace dirige a la siguiente web:

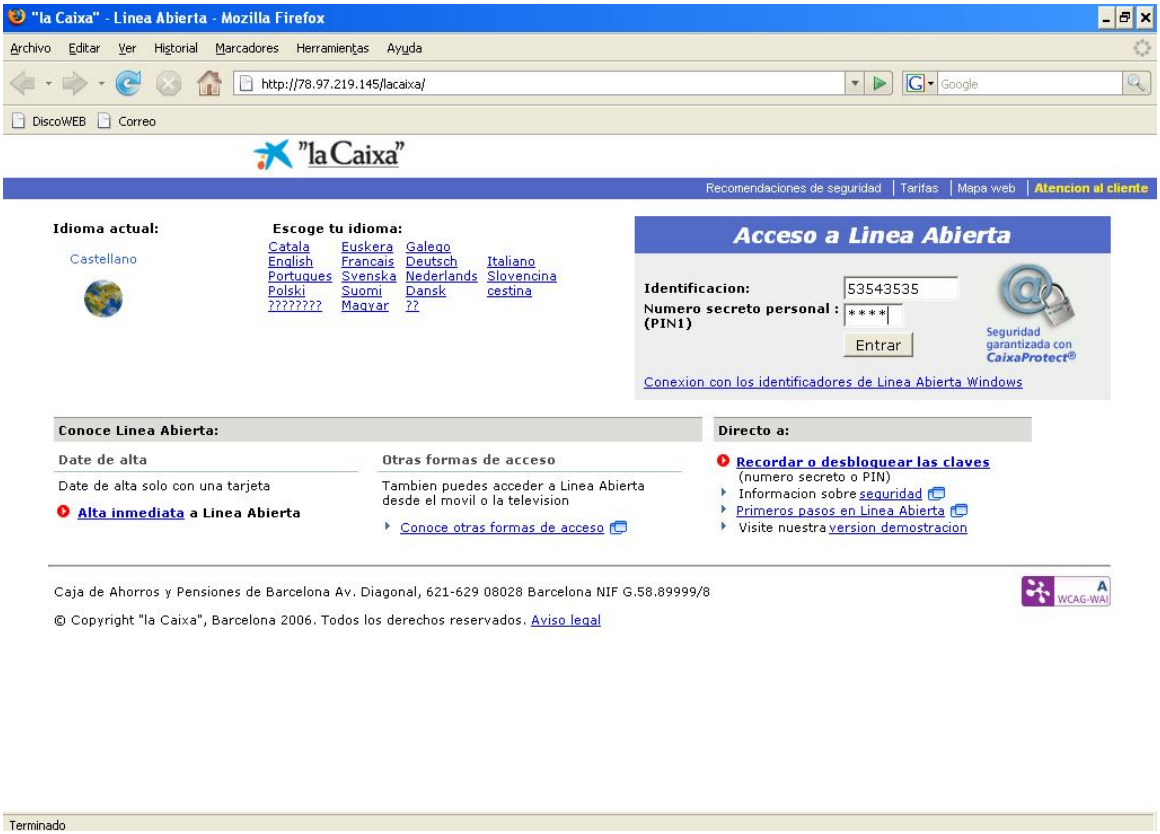


Figura 41. Scam La Caixa 1

Una vez introducido un número de identificación y clave personal, nos lleva a la siguiente página para introducir todos los datos de la tarjeta de claves:

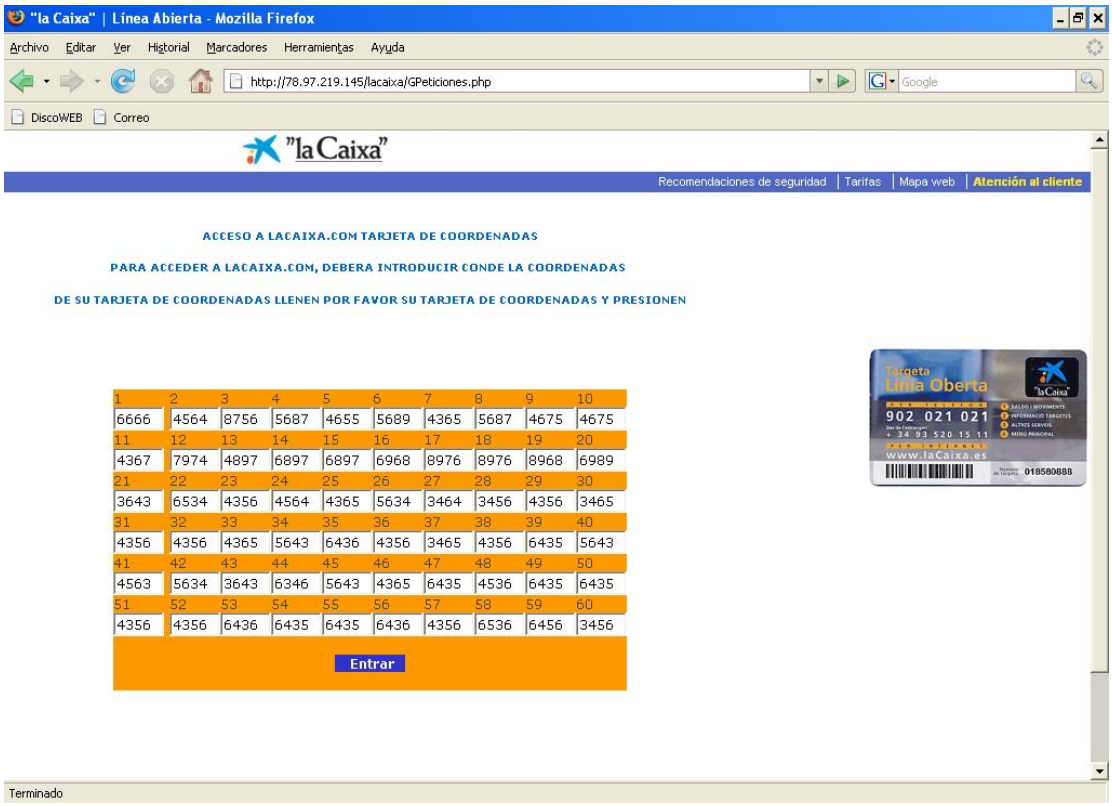


Figura 42. Scam La Caixa 2

Al introducir todas las cifras y pulsar “entrar”, automáticamente redirige a la página original de La Caixa:

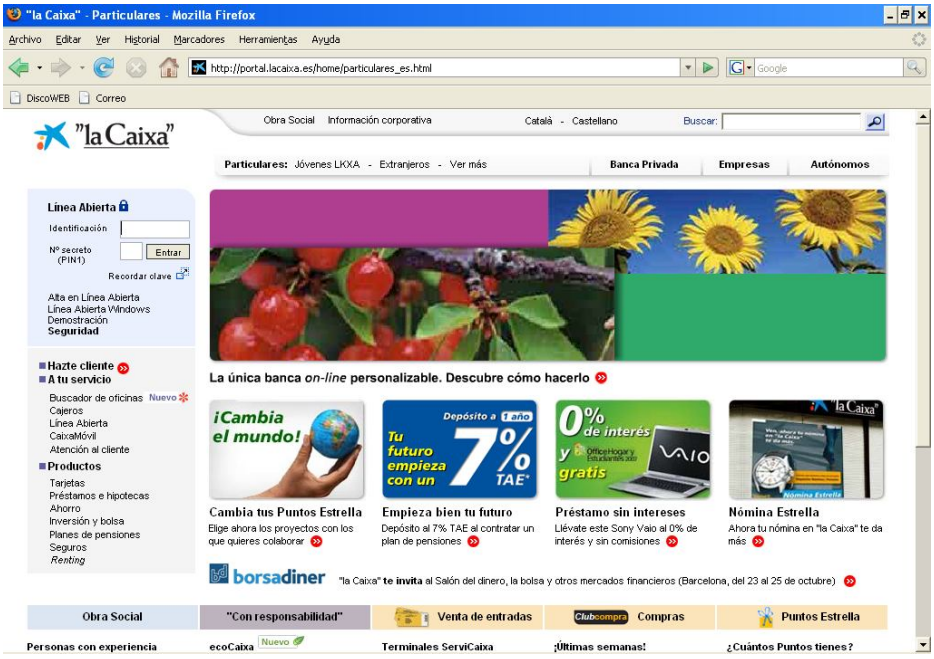


Figura 43. Scam La Caixa 3

3.4.3 Caja Madrid

El mail es:

From: Caja Madrid <fficina@cajamadrid.es>
To: fvalera@it.uc3m.es
Date: 31 Oct 2008 01:37:00 -0400
Subject: Aviso Importante!

CAJA MADRID

Notificamos que su Servicio en línea se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en línea.
Como medida de seguridad hemos decidido desactivar su cuenta temporalmente, este incidente puede deberse a que realizo intentos de acceso a su cuenta desde otra dirección IP debido a el sistema dinámico que utilizan los proveedores de Internet.
Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado :

PARTICULARES

oficina internet
CAJA MADRID

Figura 44. Correo Scam Caja Madrid

Que nos lleva a la siguiente página:

Figura 45. Scam Caja Madrid

Una vez introducido DNI, clave y firma, la página nos redirecciona a la original de Caja Madrid. Se puede observar que la página scam es idéntica a la original, salvo que añade un campo para introducir la firma (consiguiendo todos los datos necesarios para realizar cualquier tipo de transacción con esta entidad):

Figura 46. Web original Caja Madrid

3.4.4 Banco Popular

Correo:

GRUPO BANCO POPULAR [servicios@bancopopular.es]

Bankinter <http://adsl-76-208-201-20.dsl.chcgil.sbcglobal.net/popular.html>

Estimado Cliente,

Nosotros hemos determinado eso fue 5 tentativas equivocadas a la entrada en su cuenta bancaria en línea del hostname: 82-76-10-23.rdsnet.ro. Sospechamos que esta tentativa no fue legitimada así, como un medida de seguridad, nosotros hemos suspendido temporalmente su cuenta. Usted puede reactivar su cuenta, el tiempo que usted desea, verificando sus informaciones personales conectadas a su cuenta bancaria en línea.
Para reactivar su cuenta utiliza por favor chasque aquí <http://adsl-76-208-201-20.dsl.chcgil.sbcglobal.net/popular.html> .

Favor de notar:
Su cuenta se quedará suspendida para prevenir el fraude hasta que usted la reactivará.

Gracias por utilizar el servicio de Banca Electrónica.

Figura 47. Correo Scam Banco Popular

Una vez accedido al enlace, llegamos a la siguiente página web e introducimos los datos:

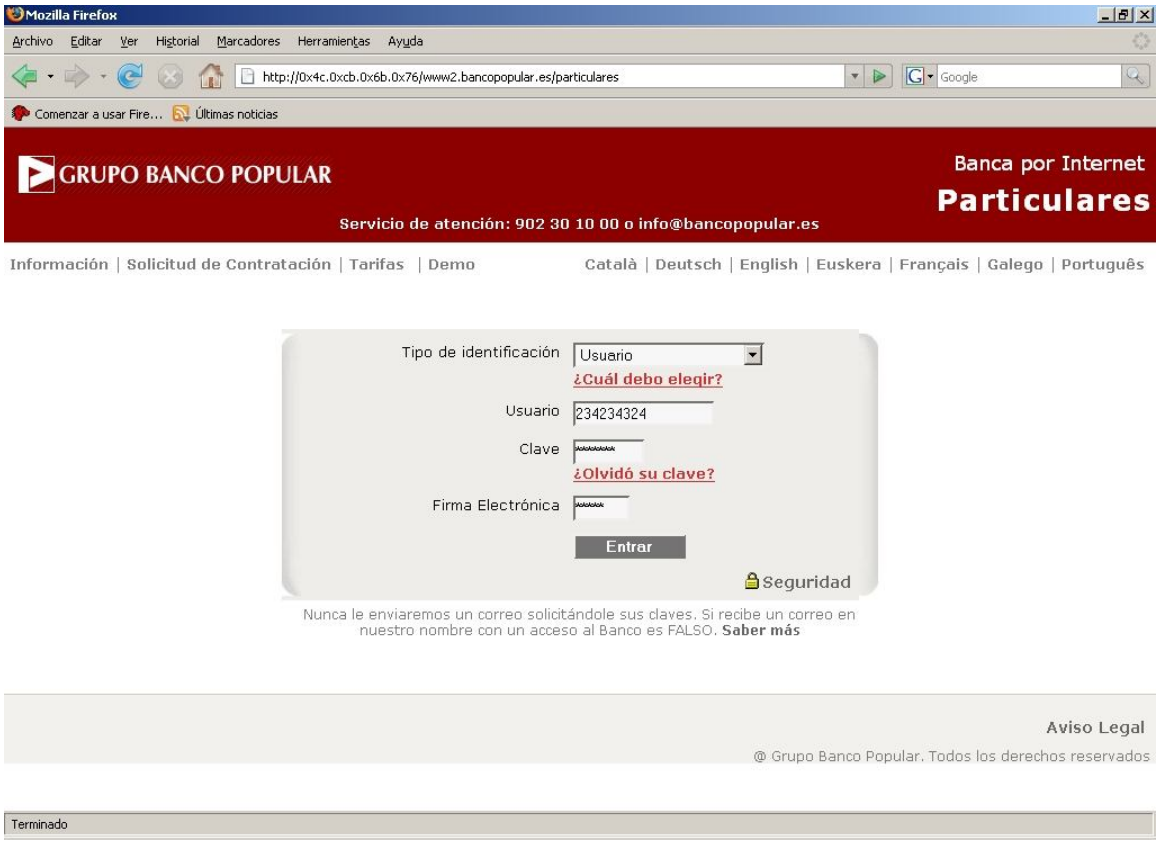


Figura 48. Scam Banco Popular

Una vez confirmados los datos, aparece la siguiente página:

Figura 49. Scam Banco Popular 2

En ella se nos muestra que ha habido un error y que para proseguir con la identificación, habrá que proporcionar más datos. Realmente, una vez finalizado este paso, los delincuentes habrán obtenido la totalidad de datos bancarios de la víctima.

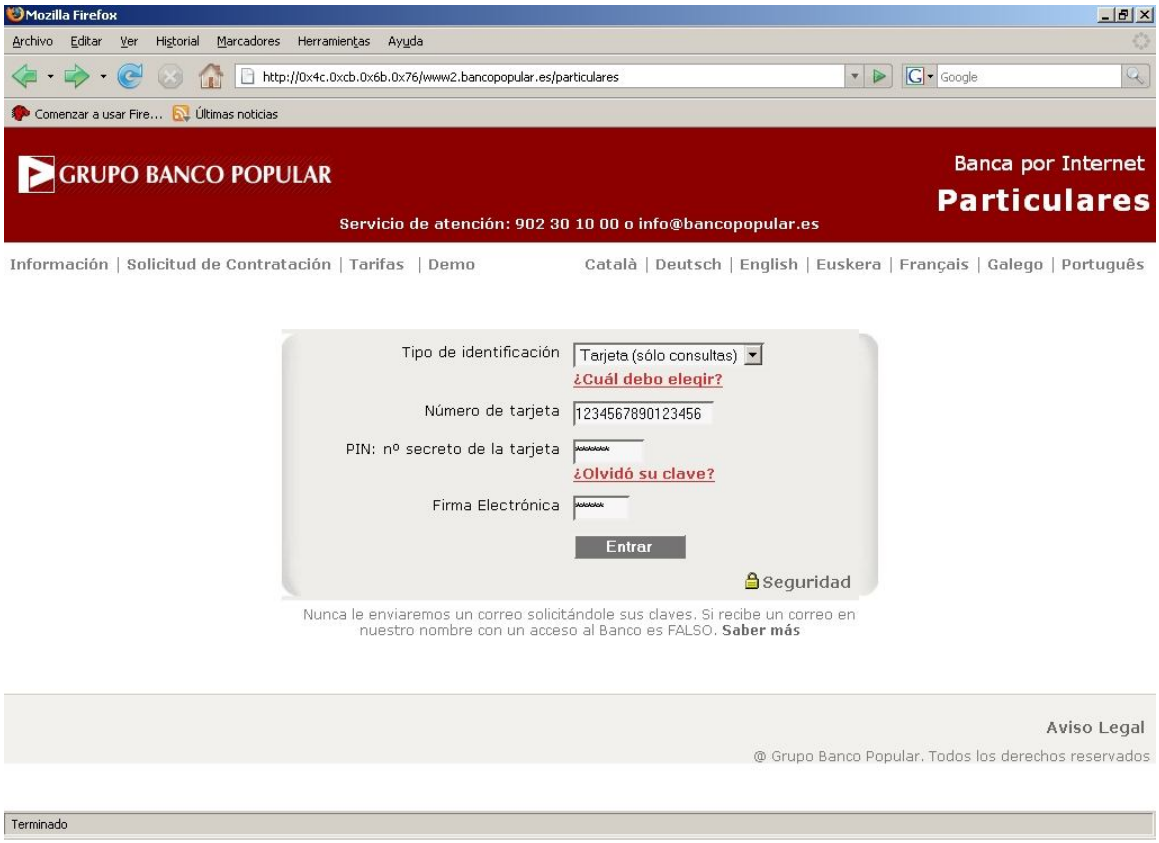


Figura 50. Scam Banco Popular 3

Para finalmente redirigirnos a la página oficial:

Figura 51. Web original Banco Popular

3.4.5 Paypal

Correo:

Dear PayPal Member,

As part of our security measures, we regularly screen activity in the PayPal system. During a recent screening, we noticed an issue regarding your account.

For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address,e-mail address).
2. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by checking the link below:
(if you can't open it just copy the link in your internet browser)

http://Paypal-accounts-update.com/index.htm

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,
PayPal Account Review Department

Figura 52. Correo Scam Paypal

Llegando al siguiente sitio, idéntico al original:

Figura 53. Scam Paypal

Aparece durante 5 segundos una página que simula que se está procesando la información y pasa al formulario de entrada de datos:

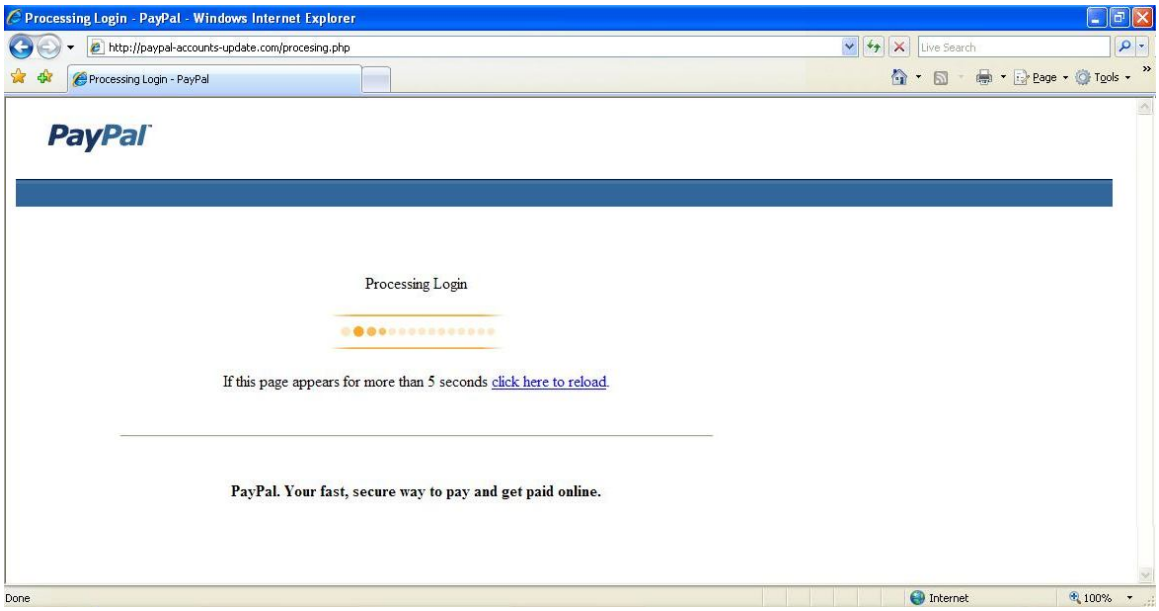


Figura 54. Scam PayPal 2

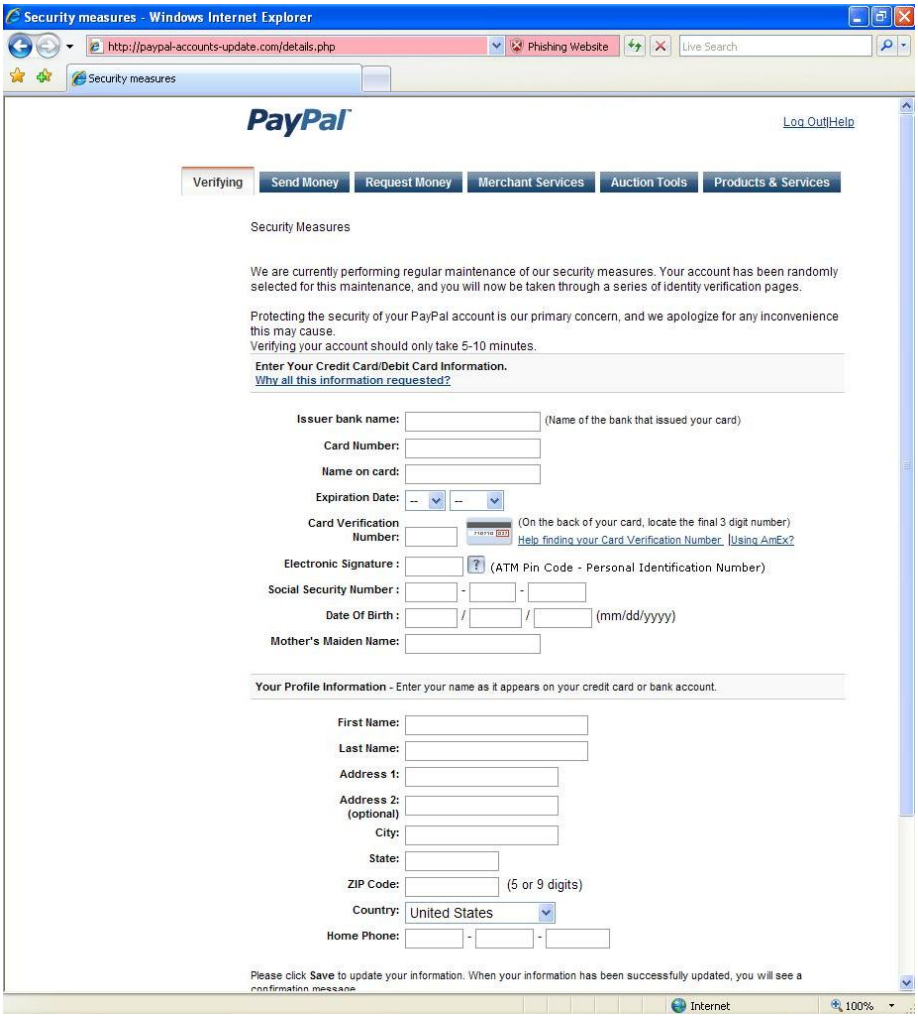


Figura 55. Scam PayPal 3

Una vez introducidos los datos en el formulario, aparece una página de confirmación y se redirige a la página oficial de PayPal:

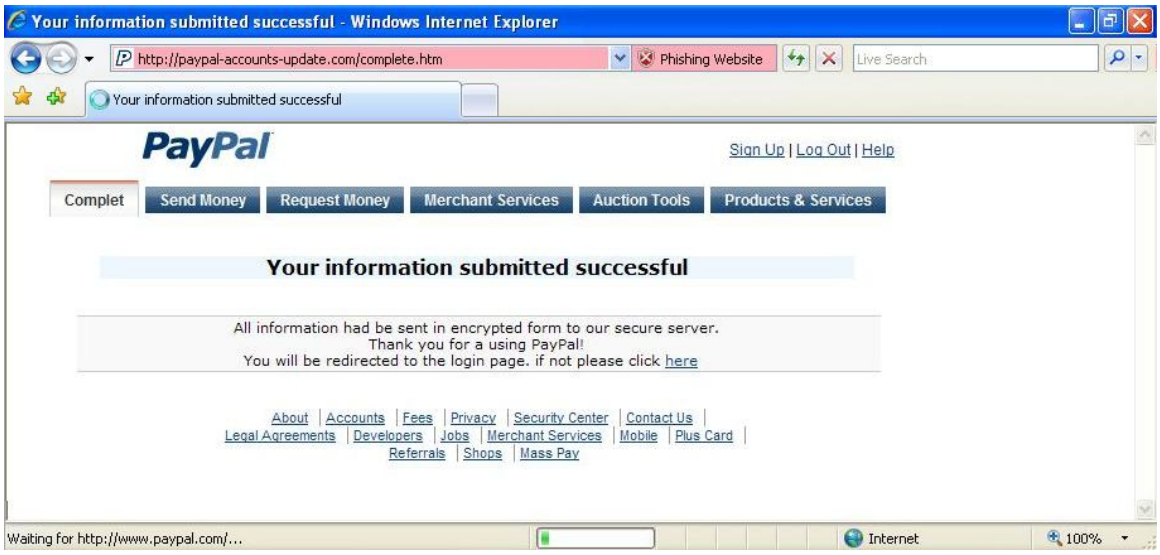


Figura 56. Scam PayPal 4

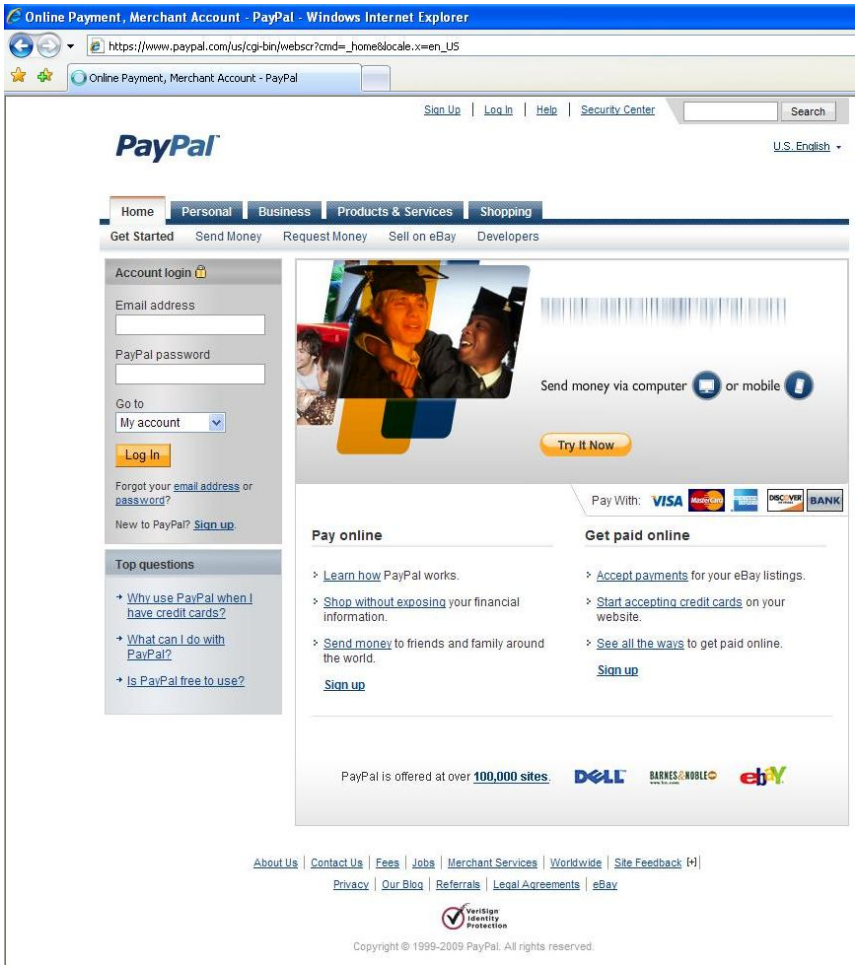


Figura 57. Web original PayPal

3.4.6 McDonald’s

Este caso difiere un poco de los demás, ya que la entidad suplantada es una empresa de comida rápida. La estafa consiste en solicitar la participación en un test de satisfacción del consumidor y ganar $80 por ello. Por supuesto, para poder acceder a ese ingreso, hay que proporcionar datos bancarios:

McDonald's Customer Satisfaction Survey
McDonald's [surveyemail@mcdonalds.eu]
martes 31/03/2009 8:46

You've been selected to take part in our quick and easy 8 questions survey

In return we will credit $80.00 to your account - Just for your time!

Please spare two minutes of your time and take part in our online survey so we can improve our services.

Don't miss this chance to change something at McDonald's.

To access the survey form please click on the link below:

http://www.mcdonalds.com/survey/ <http://ip67-155-12-123.z12-155-67.customer.algx.net/Citrix/MetaFrame/localizedContent/www.mcdonalds.com/mcdonalds.htm>

© McDonald's Customer Satisfaction Department

Figura 58. Correo Scam McDonalds

Puede comprobarse que el enlace del correo aparentemente es de la página original de la empresa, pero realmente es otro diferente. Este enlace nos lleva a un cuestionario de 8 preguntas:

Figura 59. Scam McDonalds 1

Después de contestar al cuestionario (validaba preguntas sin contestar e incluso dejarlo completamente en blanco), pasaba a una página donde se pedían los datos para poder realizar el ingreso.

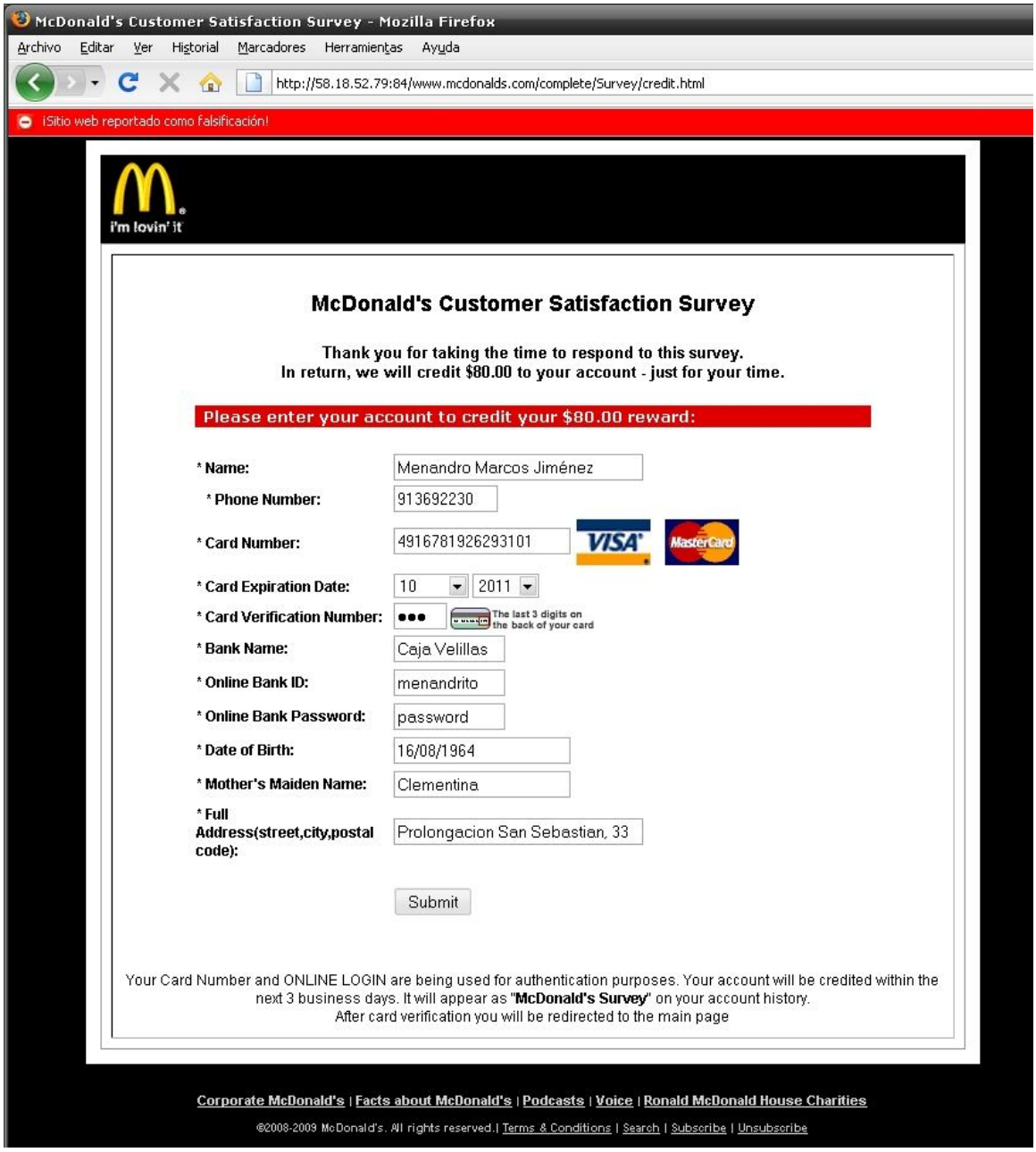


Figura 60. Scam McDonalds 2

Y finalmente ser redirigido a la página oficial de McDonalds.

En este caso se capturó la dirección IP del servidor que contenía el formulario, encontrándose este en China:

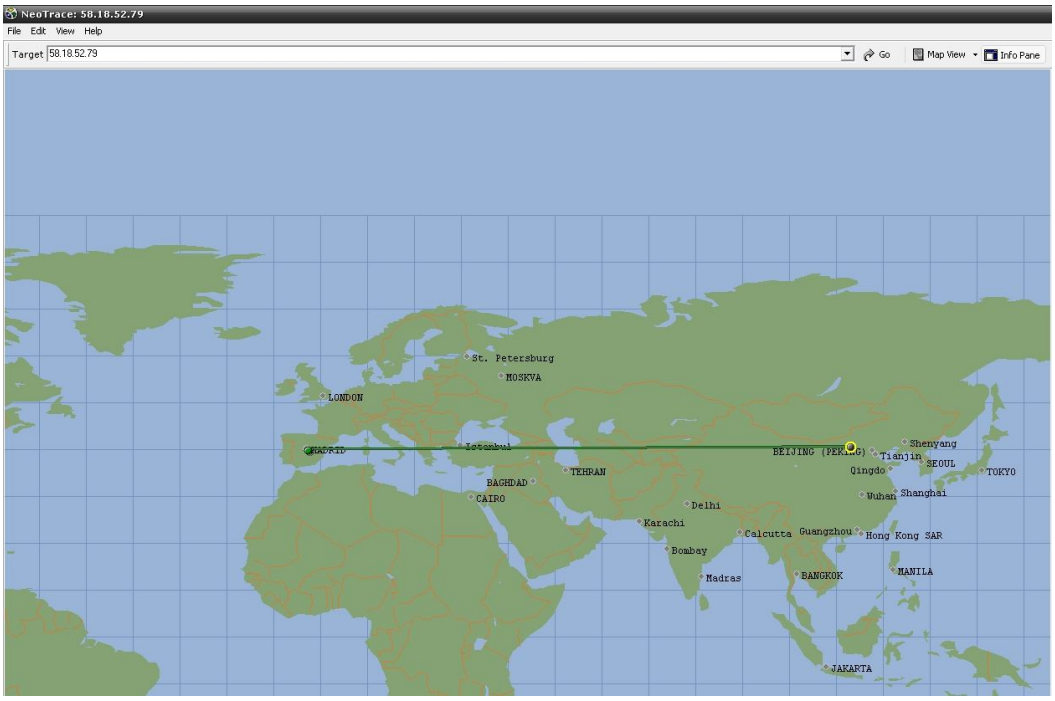


Figura 61. Mapa servidor Scam McDonalds

Y se obtuvo información sobre esa dirección IP, como el servidor donde se alojaba y el dueño:

IP Information for 58.18.52.79

IP Location:	China Beijing Cncgroup Neimeng Province Network
IP Address:	58.18.52.79 W R P D T
Blacklist Status:	Clear

Whois Record

```
inetnum:      58.18.0.0 - 58.18.255.255
netname:      CNCGROUP-NM
descr:        CNCGROUP Neimeng Province Network
descr:        China Network Communications Group Corporation
descr:        No.156,Fu-Xing-Men-Nei Street,
descr:        Beijing 100031
country:      CN
admin-c:      CH455-AP
tech-c:       HY690-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CNCGROUP-NM
descr:        CNC Group CHINA169 Neimeng Province Network
role:         CNCGroup Hostmaster
e-mail:       abuse@cnc-noc.net

address:      No.156,Fu-Xing-Men-Nei Street,
address:      Beijing,100031,P.R.China
nic-hdl:      CH455-AP
phone:        +86-10-82993155
fax-no:       +86-10-82993102
country:      CN
person:       honghui yuan
nic-hdl:      HY690-AP
e-mail:       oo@public.hh.nm.cn

address:      NO.169 hulun south road Huhhot Inner Mongolia, 010028
phone:        +86-471-6268961
fax-no:       +86-471-6291559
country:      cn
```

Figura 62. Info servidor Scam McDonalds

3.4.7 Caixa Brasil

Este caso es especial, pues en vez de llevar el enlace a una página web scam, descarga un ejecutable que se hace pasar por una aplicación para actualizar los datos. Se va a tratar en este apartado, pues a pesar de ser un ejecutable, no se trata de malware, ya que es una simple aplicación que realiza exactamente la misma función que una página web scam.

El correo, en portugués, nos indica:

Prezado Cliente,

Foi lançada uma nova correção para o Cadastramento de Computadores, esta corrige uma falha de nível crítico do sistema de identificação do cliente, que pode ocasionar perdas de dados e problemas no acesso.

A atualização é simples e rápida, basta clicar no link abaixo e em seguida completar todos os dados que pedirão para efetuar uma atualização completa.

http://www.caixa.gov.br/cadastramento/Cadastramento_de_Computador

Atenção: Todos os usuários devem se cadastrar e atualizar o Cadastramento de Computadores. Caso a correção não seja realizada, seu computador será **bloqueado e o desbloqueio só poderá ser realizado nas agências da CAIXA.**

Em caso de dúvidas, ligue para o Help Desk CAIXA 0800 726 0104

Figura 63. Correo Scam Caixa Brasil

El enlace aparentemente pertence al banco original, pero realmente nos lleva a *http://200.111.155.122/squid/monthly/.../Cadastramento_de_Computador.exe*. Con un programa trazador de rutas, averiguamos que este archivo se aloja en un servidor en Santiago de Chile:

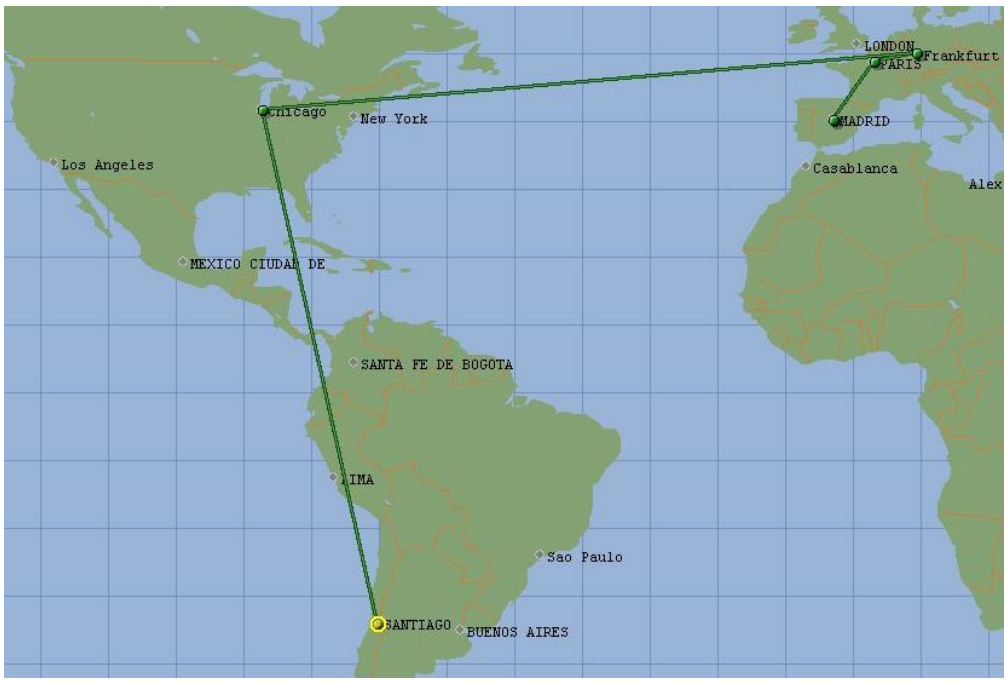


Figura 64. Scam Caixa Brasil. Alojamiento archivo

Una vez descargado el programa, se ejecuta y se abre la siguiente ventana:

Figura 65. Scam Caixa Brasil

Al pulsar sobre “iniciar actualización”, aparecen pantallas para introducir los datos:

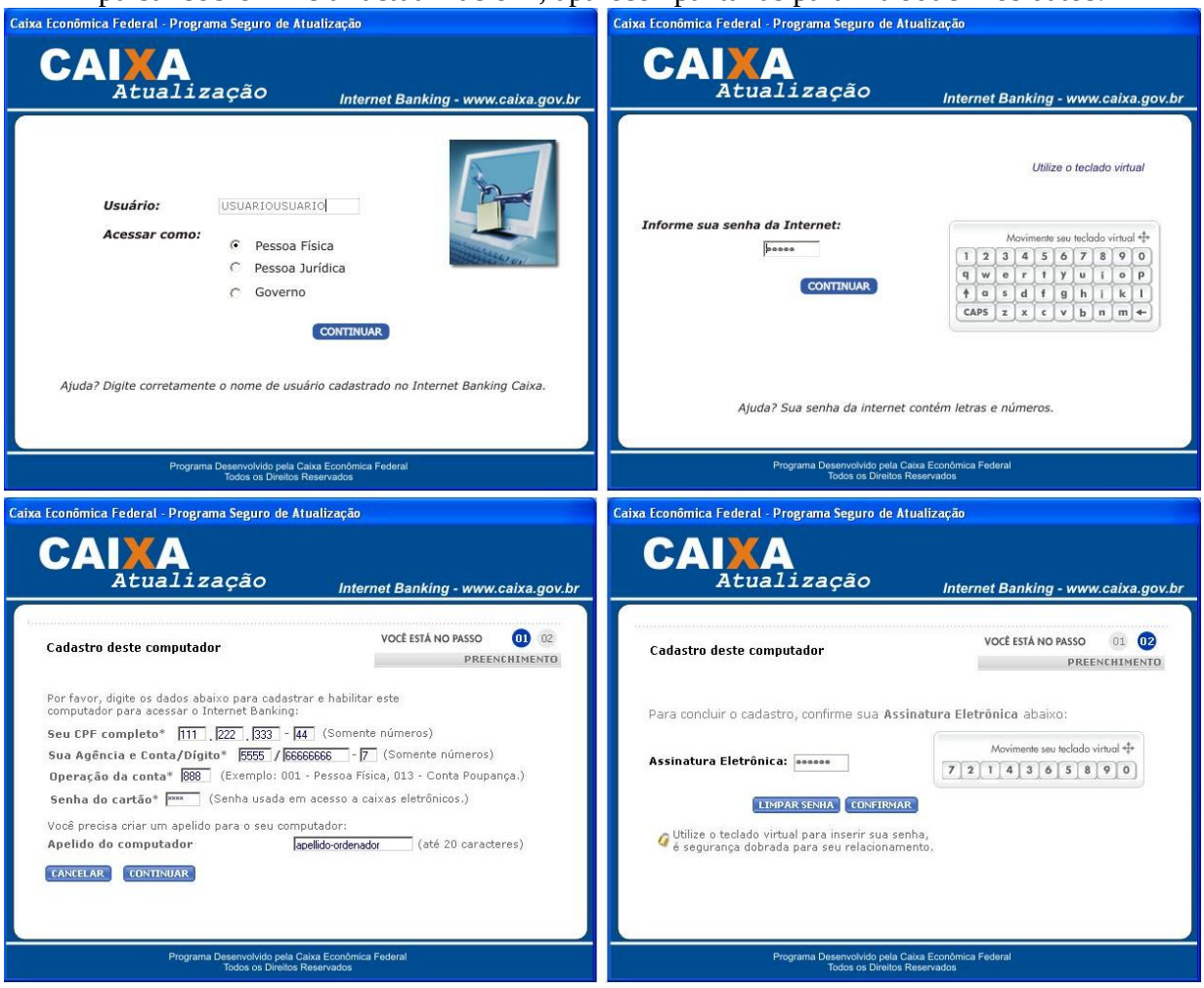


Figura 66. Scam Caixa Brasil 2

Una vez introducidos todos los datos, se abre una ventana de confirmación y al pulsar “OK”, el programa se cierra. En ese preciso momento, se captan con un analizador de redes una serie de tramas:

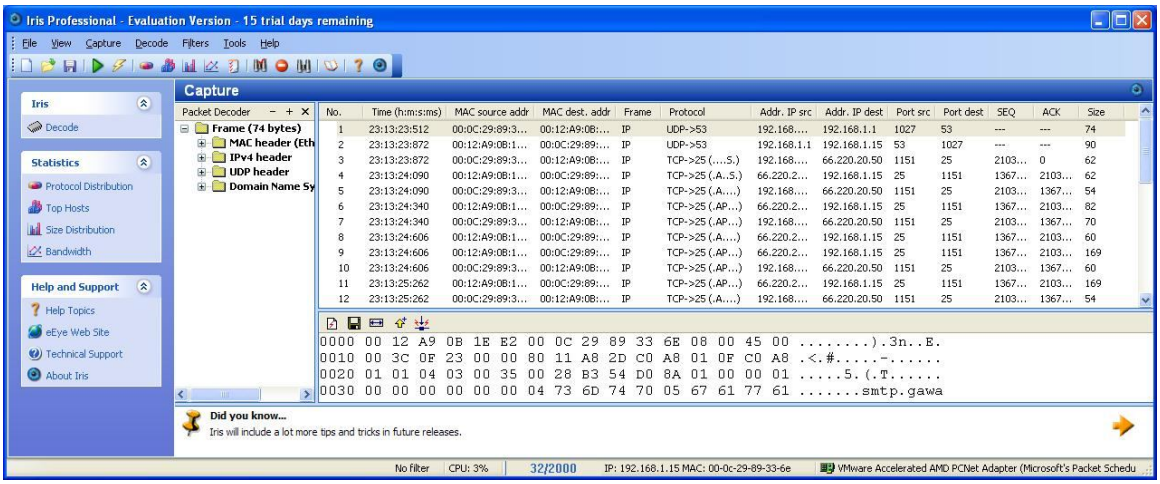


Figura 67. Scam Caixa Brasil 2. Captura tramas

Al decodificar esas tramas, descubrimos un diálogo SMTP, que no es más que un correo electrónico que se envía a la dirección *ffecsm@gawab.com*, con todos los datos previamente introducidos:

From: +Love
To ffecsm@gawab.com
Date: Monday, March 30, 2009 9:00PM
Subject: ++Brankelihna

User
00-0C-29-89-33-6E
1039D499
C:\Windows uE WINXPEN-1
XX..: USUARIOUSUARIO
XX..: fs
XX..: contras
XX..: 123456
XX..: 111.222.333-44
XX..: 5555
XX..: 66666666
XX..: 7
XX..: 888
XX..: 9999
XX..: apellido-ordenador

Figura 68. Scam Caixa Brasil 2. Email generado

3.4.8 Conclusiones

Las páginas web scam intentan dar la imagen de las oficiales de las empresas. Normalmente se pueden detectar ciertas diferencias como pueden ser el formato de la

dirección URL (presentando variaciones con respecto a la original o incluso siendo completamente distinta), distintos caracteres de puntuación, falta de cifrado, etc.

Estas páginas van a solicitarnos credenciales bancarias de forma directa, por lo que la forma de protegerse de ellas es seguir unas pautas para comprobar la veracidad de los sitios donde nos conectamos y la necesidad de que estos nos soliciten nuestras credenciales sin haber hecho nosotros nada que las requiera.

3.5 Malware

3.5.1 Introducción

Los ataques de la escuela rusa no son tan masivos como los de la brasileña, pero sí mucho más eficaces. Esto es debido a que la ingeniería social pasa a un segundo plano, y el robo de credenciales bancarias se realiza de forma que el usuario no tenga que ser forzado a realizar ninguna acción que se le pida.

En esta sección vamos a analizar varias muestras de malware proporcionadas por la empresa Instisec. Estas muestras han sido remitidas minutos después de ser recibidas desde distintas entidades de seguridad que colaboran con ellos.

Los datos que se presentarán a continuación son el resultado de infinidad de pruebas. En el mundo del malware, se requiere de mucha rapidez a la hora de analizar muestras. Aproximadamente el 90% de las muestras han tenido que ser rechazadas después de ser analizadas, pues intentaban establecer conexiones con servidores ya cerrados, mandar correos a direcciones ya inexistentes, etc. Este hecho ha ralentizado mucho el trabajo y obligado a desechar mucho tiempo dedicado, no obstante demuestra lo rápido que actúan las autoridades a la hora de detectar fraudes y cerrar cuentas y servidores maliciosos.

3.5.2 Herramientas utilizadas

Para el análisis del malware, se han utilizado herramientas muy variadas para poder supervisar todo lo que ocurre una vez ejecutado. Para el análisis de cada muestra ha habido que combinarlas todas para poder buscar indicios del comportamiento del software.

La mayoría de las veces ha habido que desechar las muestras ya que no se podía detectar ningún comportamiento extraño. Esto es debido a que no siempre tienen un funcionamiento inmediato y actúan con un temporizador o esperando a que les llegue una orden desde fuera. En este último caso, simplemente abren un *socket* y quedan a la espera.

Para poder analizar las muestras desechadas, habría que dejar máquinas monitorizadas durante el tiempo preciso a la espera de alguna actuación o decompilarlas.

Estos procesos quedan fuera de los objetivos de este proyecto, por lo que se presentarán las muestras que manifiesten un comportamiento instantáneo al ejecutarlas.

A continuación vamos a presentar las herramientas utilizadas conjuntamente:

3.5.2.1 VMWare

Gestor de máquinas virtuales. Nos permite ejecutar el malware sin comprometer la integridad de la máquina real, permitiendo realizar muchas ejecuciones en poco tiempo, volviendo a estados previamente salvados con gran rapidez.

3.5.2.2 Virus Total

Herramienta web que realiza un análisis de primer nivel de archivos sospechosos. Hace uso de más de 40 motores de antivirus, tales como *Avast*, *Kaspersky*, *McAfee*, *NOD32*, *Panda*, *TrendMicro*, etc. Gracias a esta página web, se puede subir la muestra y al cabo de un minuto ver cuántos motores detectan algo malicioso en el código, el nombre de virus que le asigna cada uno e información como el tipo de archivo que es y librerías *dll* que importa.

Toda esta información permite tener indicios para saber si la muestra se cataloga como una tipo *banker*, *keylogger*, etc. De esta forma se puede elegir qué observar con otras herramientas.

3.5.2.3 InstalWatch Pro

Este programa realiza una fotografía del sistema antes y después de ejecutar un archivo de instalación y muestra lo que ha sido añadido, modificado y borrado en el registro. Dependiendo de qué registros se modifiquen, podemos obtener indicios sobre el tipo de comportamiento que tiene la muestra a analizar.

3.5.2.4 Wireshark

Analizador de paquetes. Permite capturar todas las tramas que circulan por la interfaz de red de la máquina virtual y decodificar multitud de protocolos. A pesar de que la mayoría de las muestras que establecen conexiones de datos con servidores utilizan cifrado o un protocolo propio y desconocido, en muchas ocasiones se pueden ver claramente consultas DNS, descargas de archivos desde ciertas direcciones, y sobre todo, aunque no se pueda siempre comprobar qué tipo de datos ocupan el tráfico, ver a qué servidores se conecta el equipo.

3.5.2.5 Process Explorer

Explorador de procesos mucho más avanzado que el administrador de tareas de *Windows*. A la lista de procesos, consumo de CPU y PID de cada proceso se le añaden funciones como monitorización de suprocesos, descripción, servicios que utiliza, etc.

3.5.2.6 Neo Trace Pro

Muestra las rutas que se establecen en las conexiones. Al introducir una dirección IP muestra gráficamente en un mapa geográfico la ruta que se establece con la información de cada nodo intermedio.

3.5.2.7 File Monitor

Permite ver y capturar todos los accesos a ficheros que realiza el sistema operativo, así como el proceso que solicita esos accesos. Muy útil para detectar qué archivos lee la muestra a estudiar y si realiza alguna modificación de registros.

3.5.3 Waledac Trojan Spybot

Esta muestra fue detectada como maligna por el 74% de los motores de antivirus. Una vez ejecutada, realiza modificaciones en diferentes entradas del registro para poder autoejecutarse cada vez que se inicie el equipo.

Una vez asegurada su ejecución, escanea todos los archivos del disco duro con extensiones que se refieran a texto, es decir, *doc*, *html*, *eml*, *inf*, *log*, etc. Archivos con extensiones que no contienen texto, como pueden ser *exe*, *bmp*, *jpg*, *dll*, *avi*, *mp3*, *wav*, *zip*, etc son ignorados, lo que demuestra que el troyano está buscando direcciones de correo electrónico contenidas en los archivos del ordenador.

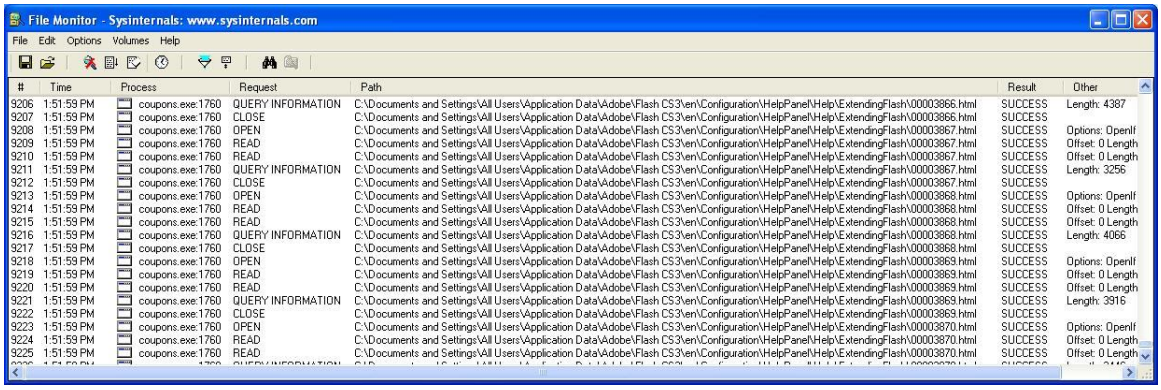


Figura 69. Waledac Trojan Spybot. Búsqueda direcciones correo

Según va escaneando el disco duro, se van escribiendo datos en un archivo HTML con nombre aleatorio y contenido cifrado. Este archivo contendrá información de interés y una vez escaneados todos los archivos del disco duro, se envía usando el comando *POST* de *HTTP*.

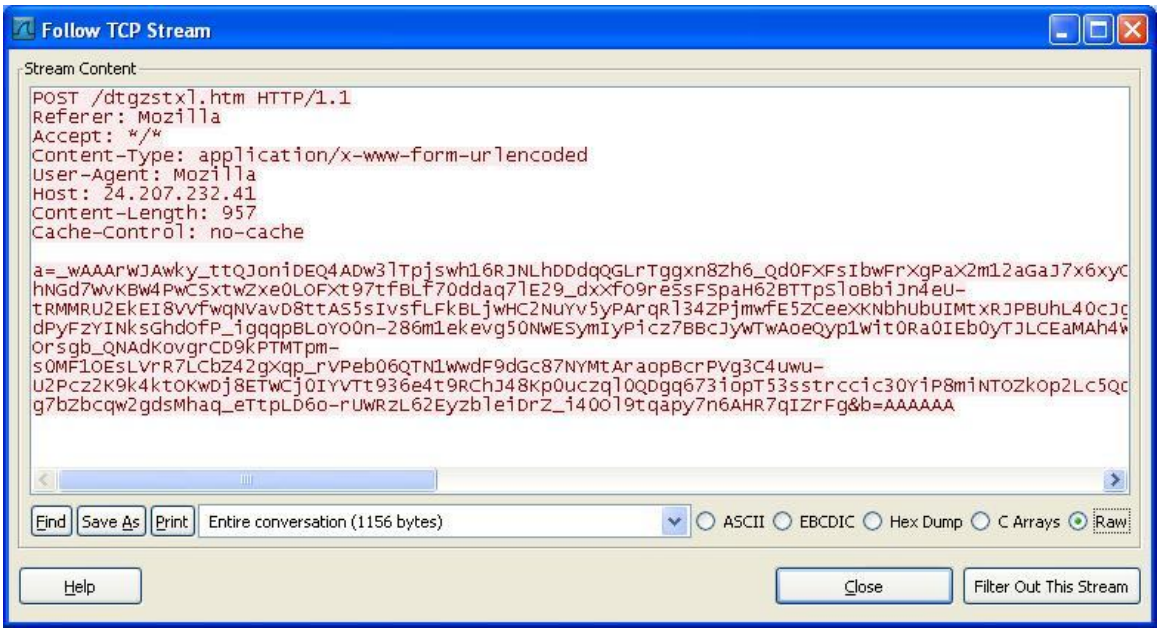


Figura 70. Waledac Trojan Spybot. Envío archivo

Una vez realizado esto, el equipo pasa a transformarse en un servidor de correo. Comienza a enviar correos spam masivamente en un bucle infinito. Una vez reiniciado el ordenador, sigue en este estado.

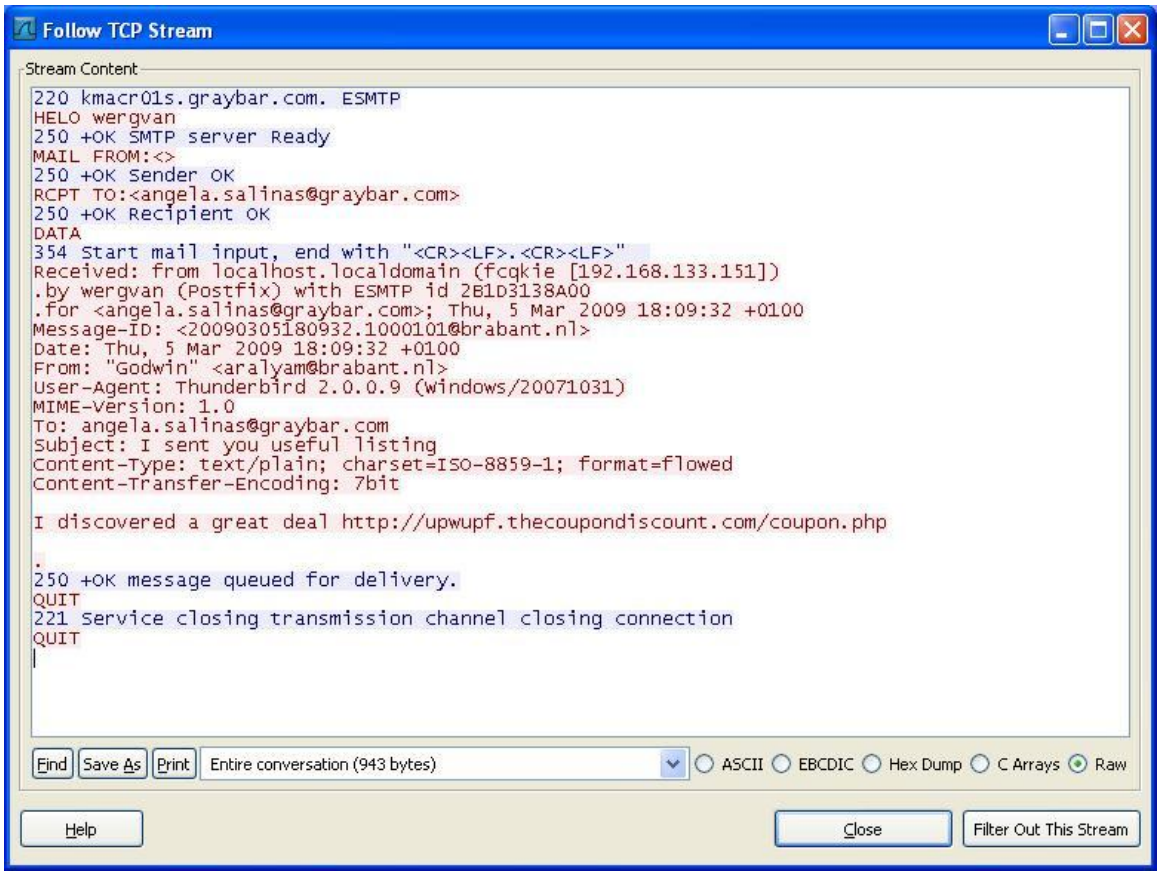


Figura 71. Waledac Trojan Spybot. Envío correos

Las direcciones de correo a las que realiza los envíos forman parte de una base de datos incluida en el archivo infectado. Más del 90% de los correos son rechazados por los servidores destino, a veces porque la dirección del remitente está en blanco (se cataloga directamente como spam) y otras veces una vez se ha realizado el envío de los datos del correo y el servidor destino, ya sea por enlace que presenta el correo o por el contenido del asunto, lo cataloga como correo no deseado y rechaza el correo antes de finalizar el envío.

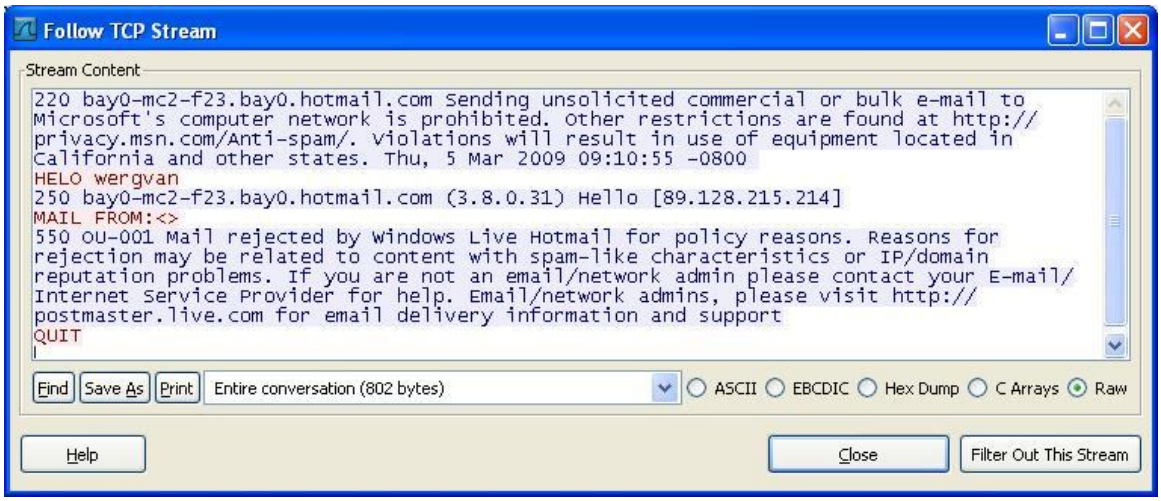


Figura 72. Waledac Trojan Spybot. Correo rechazado

El contenido de los correos es simplemente un asunto aleatorio para llamar la atención y un enlace a una dirección de dominio que pertenece a un conjunto de dominios muy reducido y subdominio aleatorio, que lleva a abrir una página php desde la que se descarga el troyano.

Esta muestra es un ejemplo de un troyano que capta direcciones de correo, las reenvía a una base de datos remota y además transforma la máquina infectada en un servidor de correo que hará uso de las direcciones que se han ido recolectando gracias a otras máquinas infectadas, para así poder ir expandiéndose.

Este mismo sistema se utiliza para enviar correos phishing con enlaces a páginas web scam, de forma que tanto los servidores de correo como los buscadores de direcciones válidas están dispersados por todo el mundo y sería imposible interceptar todos.

3.5.4 Sramler Spybot Backdoor

Este archivo al ser ejecutado se graba en /windows/system con otro nombre y acto seguido el archivo inicial se borra. Este nuevo archivo realiza modificaciones en el registro para autoejecutarse cada vez que se inicie el equipo.

Su funcionamiento real no comienza hasta una vez reiniciado el equipo, momento en el cual, realiza una conexión con la dirección IP 65.60.44.146 en el puerto 81 sin mostrarse ningún tráfico durante horas. Aparentemente esta conexión abierta queda a la espera de comandos desde el servidor para realizar operaciones de espionaje en el equipo infectado.

3.5.5 Sinowal

Al ejecutarse, lee y borra las *cookies* del ordenador. También lee los archivos favoritos del *Internet Explorer* e información de las cuentas de correo de *Outlook.*

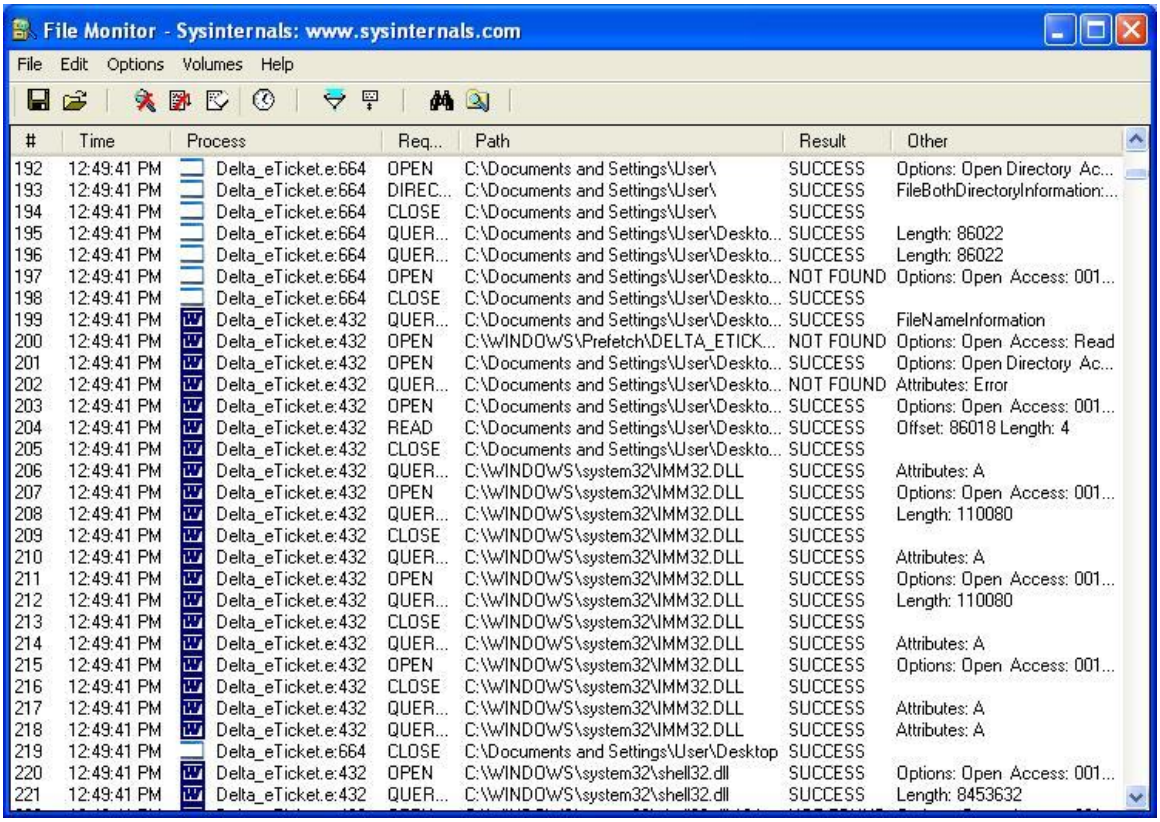


Figura 73. Sinowal. Lectura de archivos

A continuación realiza un intercambio de datos con un servidor en Estonia y otro en Ucrania. Estos datos van cifrados, por lo que únicamente se puede saber el destino de estos.

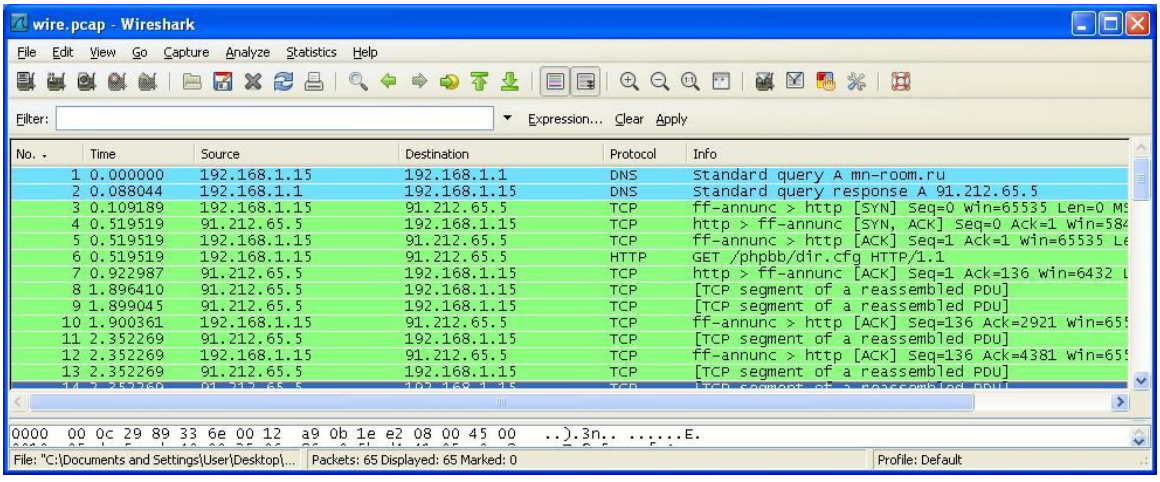


Figura 74. Sinowal. Captura de tramas

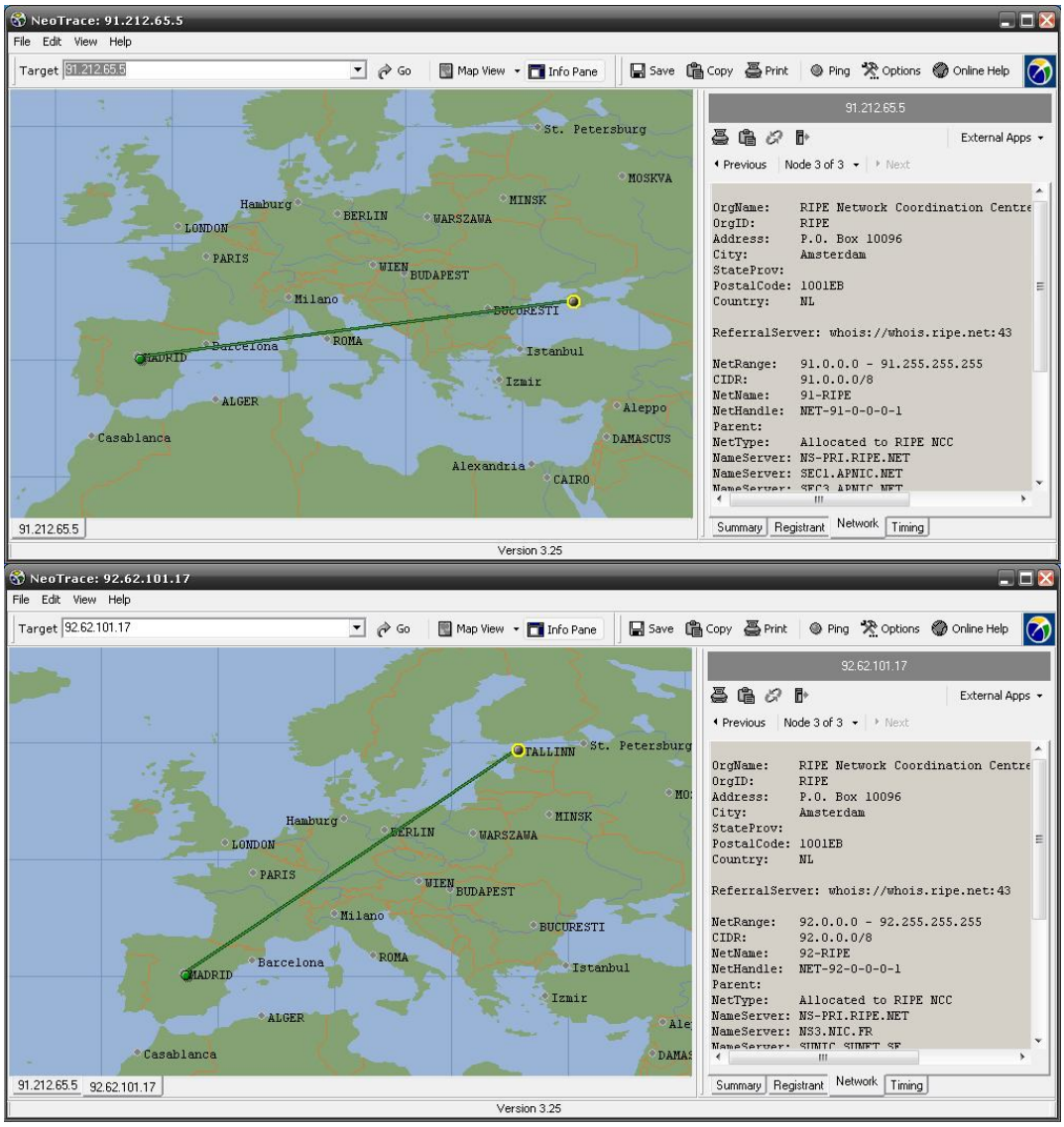


Figura 75. Sinowal. Ubicación servidores de contacto

3.5.6 Papras

Esta muestra fue detectada por el 62% de los motores de antivirus.Una vez ejecutado, el archivo crea una copia idéntica de sí mismo en el directorio *Windir* con el nombre *9129837.exe* y el driver *new_dvr.sys* que sirve para ocultar su actividad. En la siguiente imagen puede observarse cómo pasa la ejecución del archivo infectado inicial (*Flash_Adobe11.exe*) a *9129837.exe*.

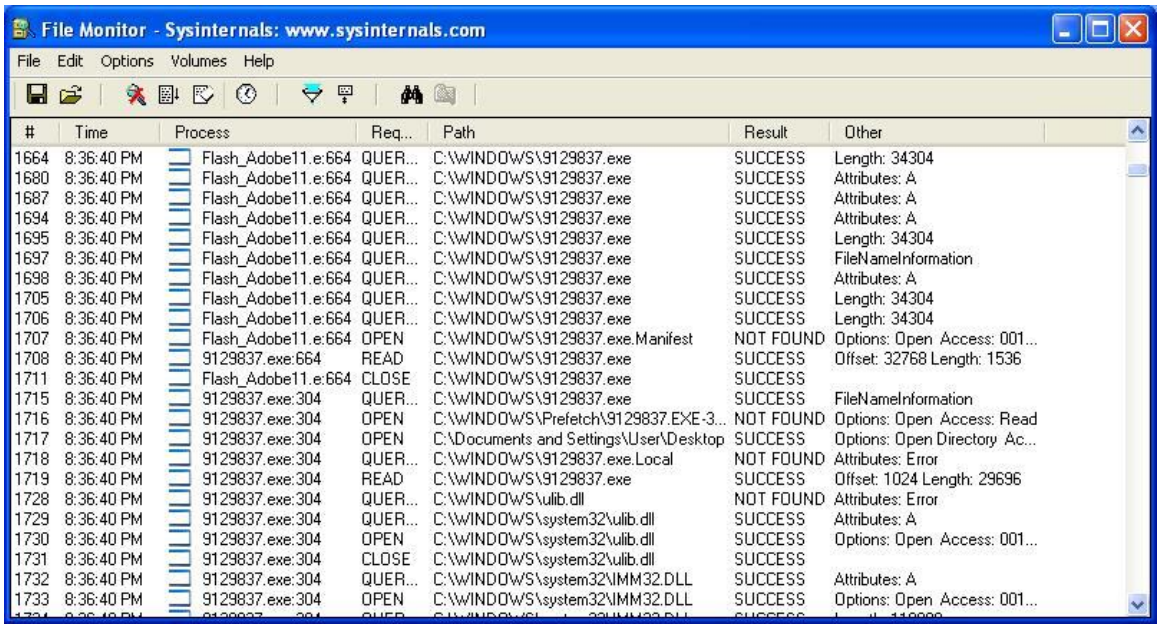


Figura 76. Papras. Cambio de archivo de ejecución

Realiza diversas lecturas y modificaciones en el registro de *Windows*, y pasa a tomar control de diversas funciones como *CreateProcess*, *HttpSendRequest*, *InternetReadFile*, etc, con el objetivo de recolectar información de interés, como pueden ser credenciales de POP3, FTP, etc.

Acto seguido intenta conectar con el dominio *http://pull.dolcebrava.com* para realizar el envío de la información que va interceptando.

3.5.7 Conclusiones

El análisis de muestras de malware, al no tener indicios de lo que hacen en un principio, requiere de multitud de ejecuciones monitorizando con herramientas muy distintas. Normalmente la información que se puede obtener una vez realizada la investigación es muy reducida:

- El intercambio de datos con servidores está cifrado
- En numerosas ocasiones, el proceso intenta descargar información o contactar con servidores que ya han sido bloqueados

3.6 Otras herramientas

3.6.1 Introducción

Además de las herramientas más características del mundo del *phishing* estudiadas hasta ahora, existen muchos otros tipos de utilidad más amplia pero también muy útiles

para la consecución de los objetivos de los delincuentes electrónicos. A continuación estudiaremos algunas utilidades representativas.

3.6.2 Ghostnet

3.6.2.1 Introducción

Herramienta usada en una red de espionaje china. Tiene multitud de funcionalidades que permiten obtener una gran cantidad de información del usuario infectado. Este programa ha infectado más de 1300 equipos en 103 países. [23]

Consiste en una estructura cliente-servidor. El cliente es diseminado por la red, normalmente a través de un archivo adjunto a correos electrónicos. Una vez ejecutado en el equipo destino, este puede ser controlado a través del servidor, que mantiene una lista de todos los equipos infectados a los que se puede acceder en todo momento para realizar prácticamente cualquier tipo de operación.

El programa principal consiste en una ventana que muestra una lista de los ordenadores infectados que en ese momento tienen conexión. Se puede acceder manualmente a cada uno de ellos para realizar funciones tales como explorar sus archivos, abrir el *símbolo de sistema*, ver el escritorio de forma remota, ejecutar archivos, etc.

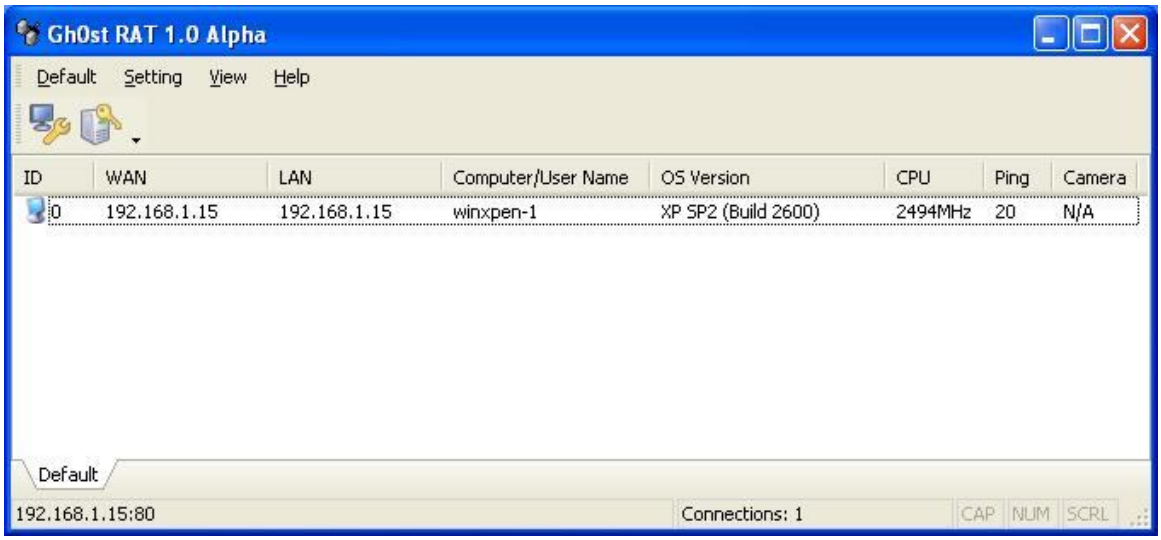


Figura 77. Ghostnet. Pantalla principal

Como se puede observar, el programa muestra en este caso un equipo infectado (en el estudio es otra máquina virtual), mostrando su dirección WAN, LAN, nombre de equipo, versión de sistema operativo, velocidad de procesador, tiempo de ping y la disponibilidad de webcam.

El propio programa presenta una función *build* que permite generar archivos ejecutables para expandir por la red e infectar ordenadores.

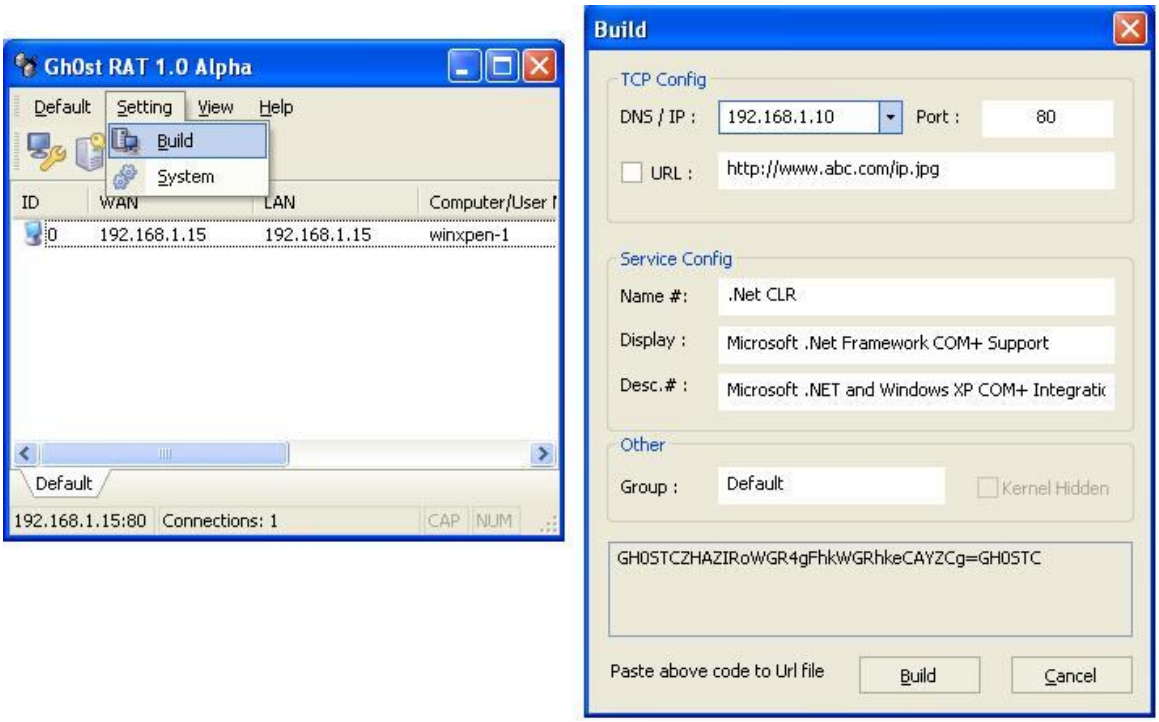


Figura 78. Ghostnet. Creación archivo infección

De esta forma se crea un archivo ejecutable llamado *server.exe*, que conecta con la dirección IP y puerto o URL que hayamos decidido. Lo más lógico para el atacante sería configurar el archivo para que conectase a la dirección del servidor en el puerto 80, de esta forma la actividad de red del equipo infectado no mostraría aparentemente ningún comportamiento anómalo, ya que la comunicación entre cliente y servidor se tomaría como tráfico HTTP.

Al capturar las tramas entre cliente y servidor al realizar la conexión o cualquier función, se puede comprobar que el tráfico de datos está cifrado, pues incluso utilizando la captura de teclado, no aparecen en las tramas los caracteres tal y como se han pulsado.

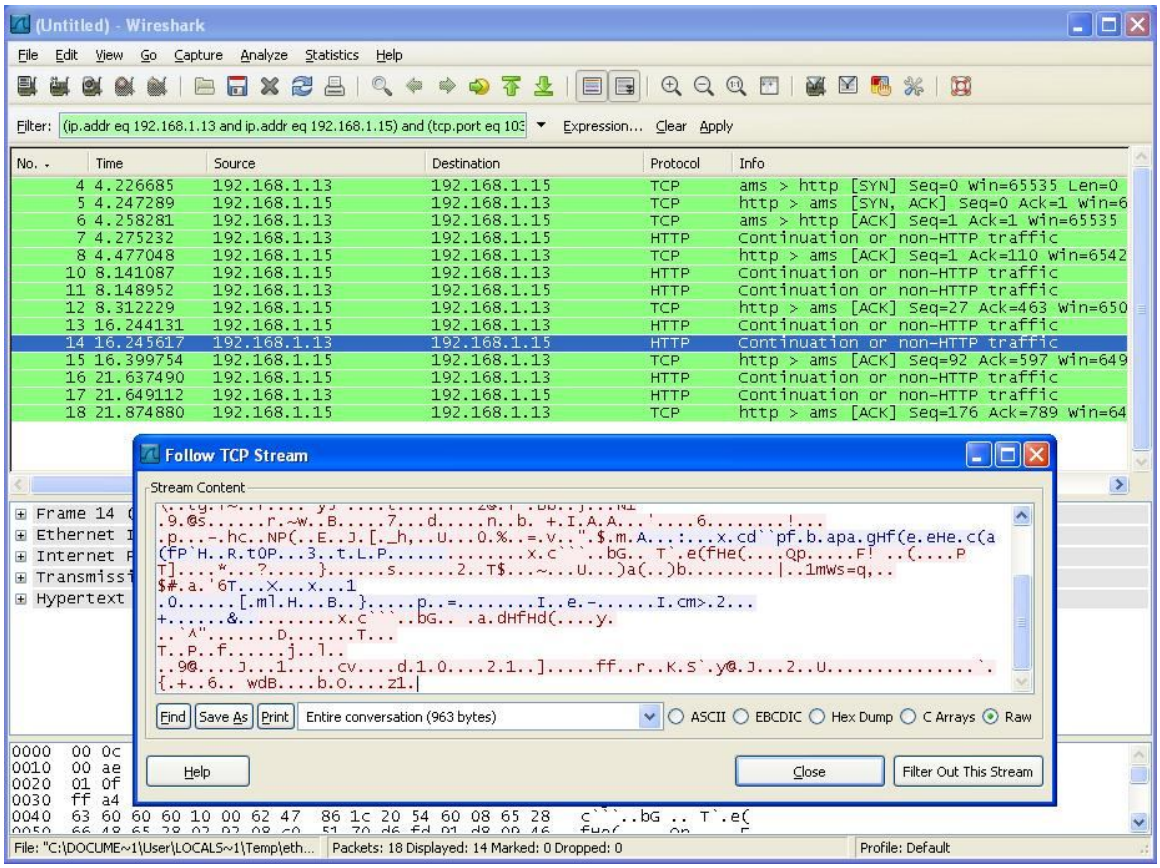


Figura 79. Ghostnet. Captura de tramas

A continuación vamos a ir viendo las herramientas de espionaje que este presenta este programa.

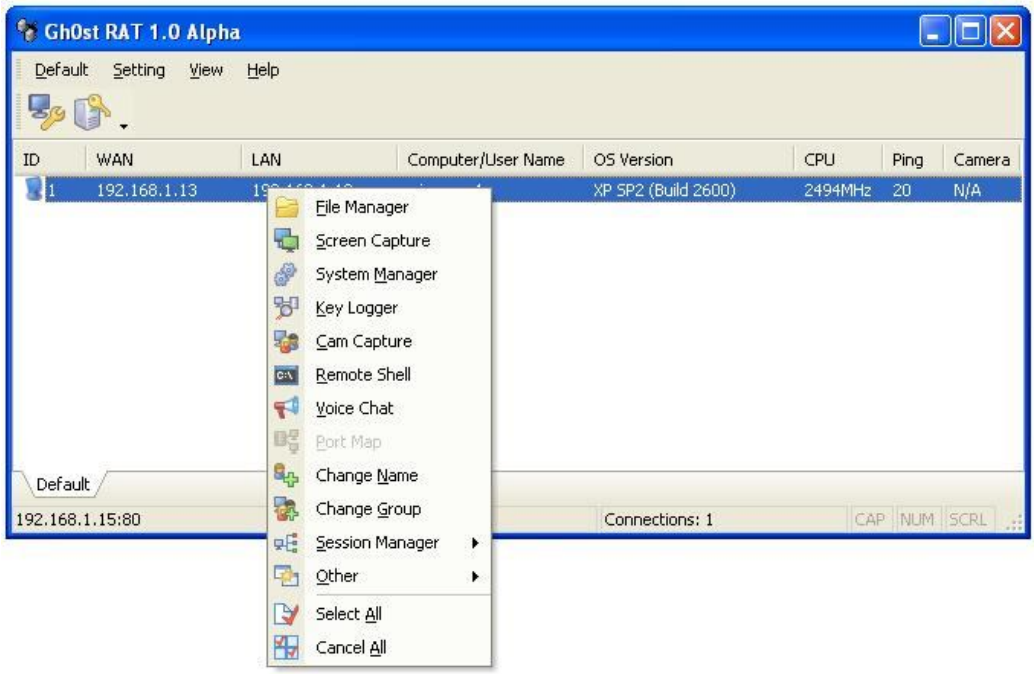


Figura 80. Ghostnet. Herramientas

3.6.2.2 Explorador de archivos

Permite al atacante usar el ordenador infectado como si fuese un servidor ftp, permitiendo manejar y arrastrar archivos del equipo remoto como si de una unidad local se tratase. Accede a todos los ficheros del disco duro teniendo un acceso total para poder leerlos, editarlos, borrarlos, crear nuevos, etc.

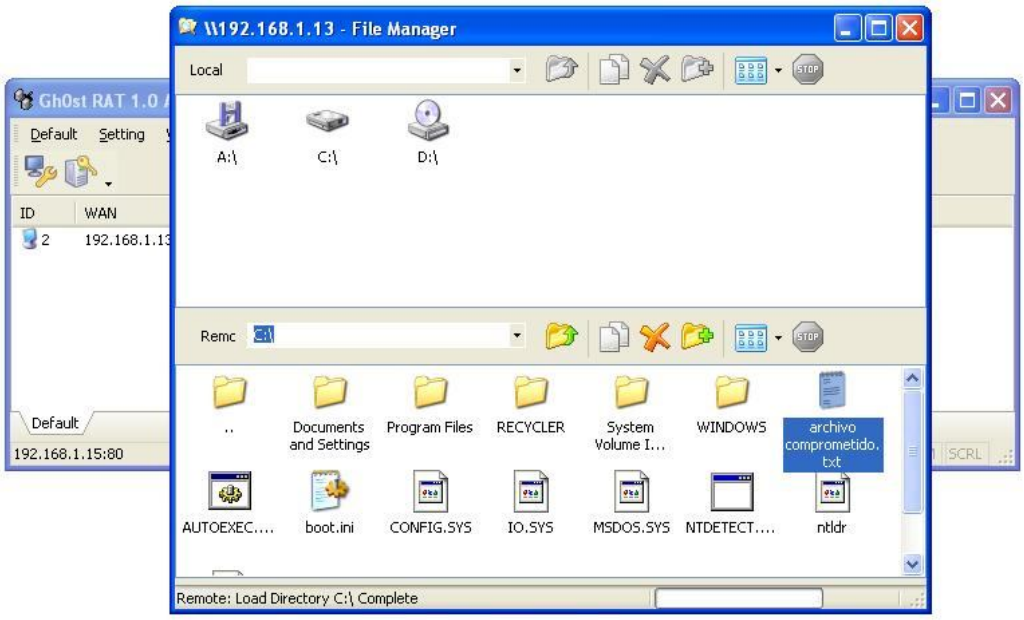


Figura 81. Ghostnet. Explorador de archivos

Esto hace posible que el atacante sea capaz de realizar multitud de acciones tales como:

- Introducir directamente *malware* en el equipo atacado para posteriormente ejecutarlo.
- Copiar archivos de información de interés, tales como correos electrónicos, libretas de direcciones, historiales de Internet, archivos de usuarios y contraseñas guardados del navegador web, etc.
- Modificar archivo de caché de direcciones DNS para redirigir páginas web bancarias a páginas *scam*.
- Modificar archivos como *autoexec.bat* o añadir enlaces en menú inicio para autoejecutar malware al iniciar el equipo
- Modificar enlaces de archivos de favoritos de navegadores web para redirigirlos a páginas *scam*.

3.6.2.3 Captura de teclado

Como ya se ha podido ver en apartados anteriores los *keyloggers* son herramientas bastante útiles para captar todo lo que se introduce por teclado. Analizando los datos recibidos, se pueden captar tecleos de *URLs* de *páginas web*, escritura de correos electrónicos y lo que es más importante, introducción de nombres de usuario y contraseñas por teclado.

Haciendo la prueba con la introducción de la dirección de la página de *banca electrónica* de *Caja España* podemos ver cómo recopila la información la herramienta *keylogger* a medida que se va tecleando en el ordenador atacado. Este es uno de los pocos sistemas que permiten adquirir contraseñas introducidas, pues normalmente en los formularios web los caracteres aparecen como círculos negros para evitar ser leidos por terceras personas.

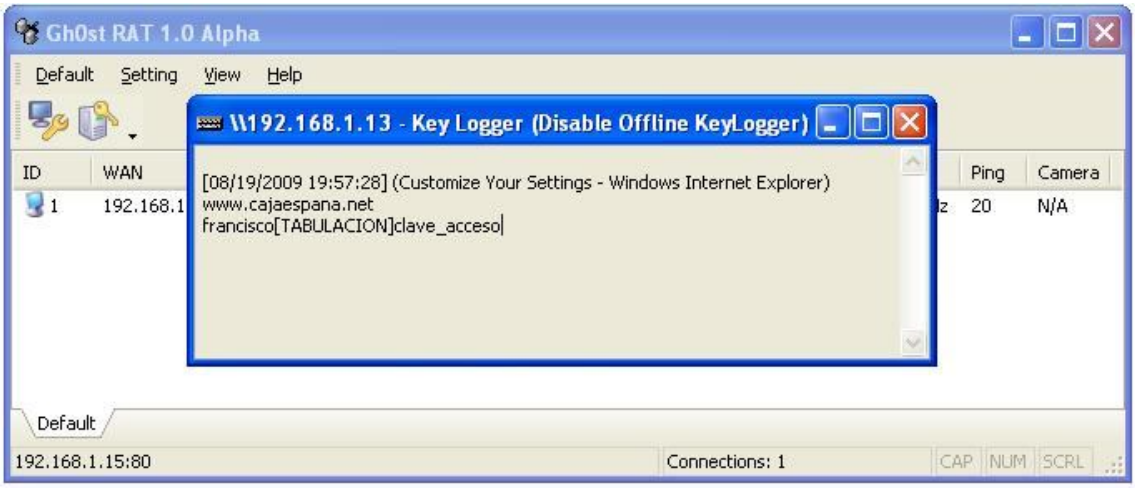


Figura 82. Ghostnet. Keylogger

Se puede comprobar que el capturador de teclado facilita el trabajo de identificación de los datos introducidos, pues junto a la fecha y hora de los tecleos, añade el nombre del programa sobre el que se está tecleando. De esta forma es sencillo saber si son datos procedentes del navegador web (introducción de direcciones, usuarios y contraseñas), edición de correos electrónicos, etc.

3.6.2.4 Capturador de pantalla (video)

Los portales web de las entidades bancarias suelen tener teclados virtuales para evitar de esa forma las captaciones de teclado. Para evitar este problema y también como herramienta visual, *Ghostnet* contiene una herramienta de captura en tiempo real que permite ver en una ventana lo mismo que el se está viendo en la pantalla del ordenador infectado. De esta forma se puede ver a simple vista el tecleo de contraseñas en teclados virtuales, páginas que se están visitando en un momento puntual, etc. Combinando esta herramienta con el capturador de teclado, se pueden obtener todo tipo de credenciales introducidas en cualquier página web.

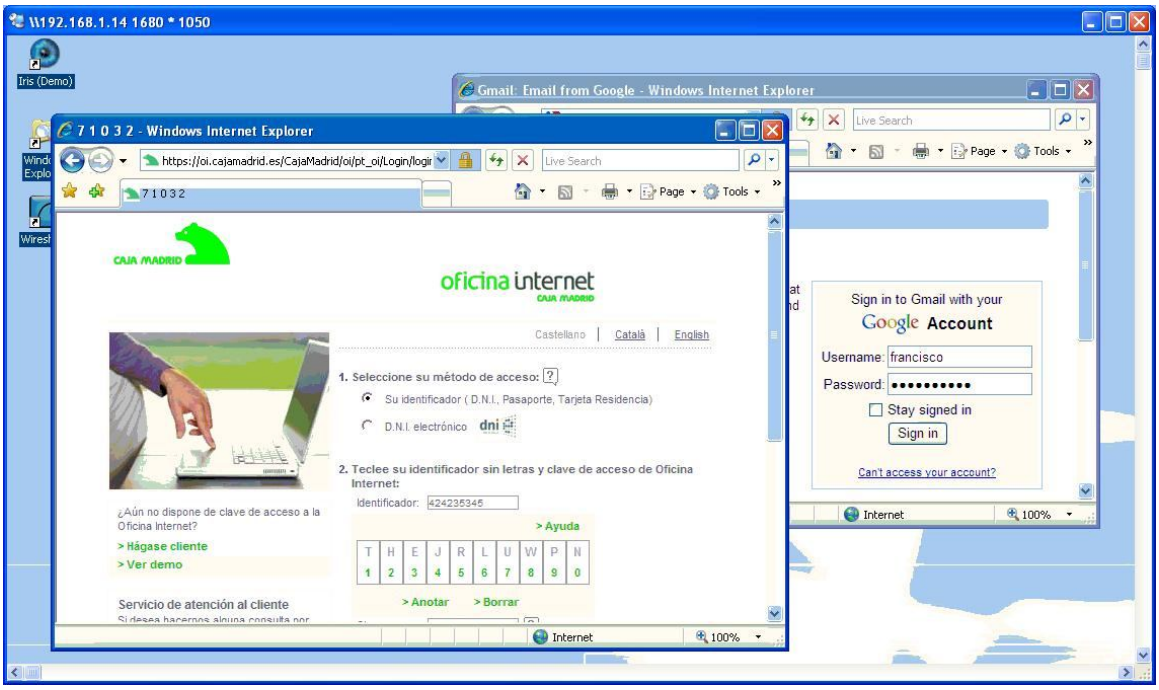


Figura 83. Ghostnet. Capturador de pantalla

3.6.2.5 Consola remota

Permite ejecutar una consola remota (*shell*). Esto es útil principalmente para ejecutar archivos, que han podido ser introducidos previamente con el explorador de archivos.

Figura 84. Ghostnet. Consola remota

3.6.2.6 Chat de voz

Esta herramienta sirve para captar entradas de audio del sistema atacado. La fuente de sonido es el micrófono del sistema, pero también permite seleccionar una entrada auxiliar o la salida de sonido del sistema entre otros.

Su utilidad está más orientada a espionaje de nivel avanzado, para algo más que simplemente obtener unas credenciales. Su uso para espionajes en reuniones de empresa o sucursales bancarias puede ofrecer información muy importante.

También puede grabar en un archivo *wav* el sonido captado y mandar mensajes de voz al equipo atacado para establecer una conversación.

Figura 85. Ghostnet. Chat de voz

3.6.2.7 Captura de cámara web

Si el equipo infectado posee una *webcam* activa, abre una ventana que muestra en tiempo real la imagen que está captando. Su utilidad para el mundo del *phishing* es relativa, aunque sí que cabe destacar el nivel de control sobre el usuario que Ghostnet brinda a un atacante al combinarlo con el resto de herramientas.

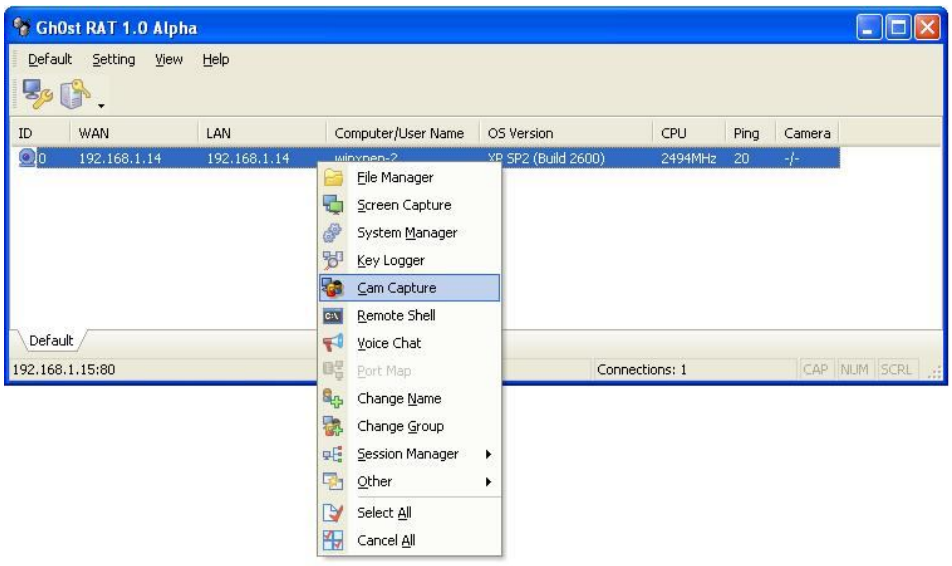


Figura 86. Ghostnet. Captura de cámara

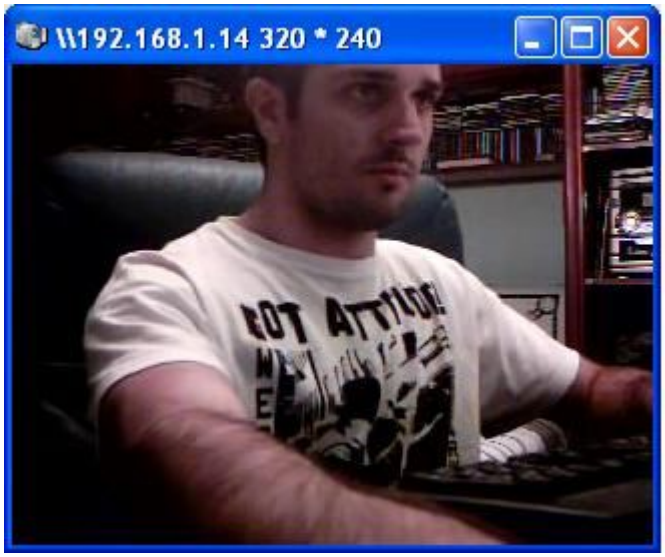


Figura 87. Ghostnet. Captura de cámara 2

3.6.2.8 Otras opciones

Hemos comentado las herramientas más importantes de *Ghostnet*. Otras herramientas menos elaboradas y de menor importancia para realizar espionaje son:

- Gestor de sistema: muestra todos los procesos activos, la ruta del archivo asociado al proceso y su *PID*.
- Modificación de nombre de equipo.
- Modificación de identificador de red.
- Gestor de sesión: permite cerrar sesión, reiniciar o apargar el equipo remotamente.
- Actualizar desde una *URL* a elegir el archivo infectado.
- Abrir una *URL* remotamente, tanto de modo normal (con el navegador predeterminado visible) como oculto.

3.6.2.9 Conclusiones

La combinación de todas las herramientas que este programa brinda, equivale a estar junto al equipo atacado captando todo lo que le rodea y sin ser visto, tener la posibilidad de usar ese equipo sin dejar rastro incluso a la vez que el propio usuario y guardar toda la información captada de forma rápida y cómoda. Todo esto se puede realizar con varias víctimas a la vez, con lo que se puede tener una idea de la capacidad de control que este programa ofrece a su usuario.

3.6.3 Fishing Bait 1.5

3.6.3.1 Introducción

Este programa permite duplicar páginas web de forma que los contenidos de los campos que sirven para introducir datos como pueden ser nombres de usuario o contraseñas sean subidos a la dirección que el usuario quiera. En definitiva, es un generador de páginas *SCAM*.

No es una herramienta muy sofisticada, pues estas modificaciones se pueden realizar manualmente teniendo unos conocimientos básicos de programación, pero supone un ejemplo de los programas que permiten realizar delitos informáticos sin necesidad de tener grandes conocimientos técnicos.

3.6.3.2 Funcionamiento

Al iniciar el programa, se abre una ventana sobre el que se pega el código fuente de la página web a duplicar. En este caso ponemos el código *HTML* de la página web de Caja España.

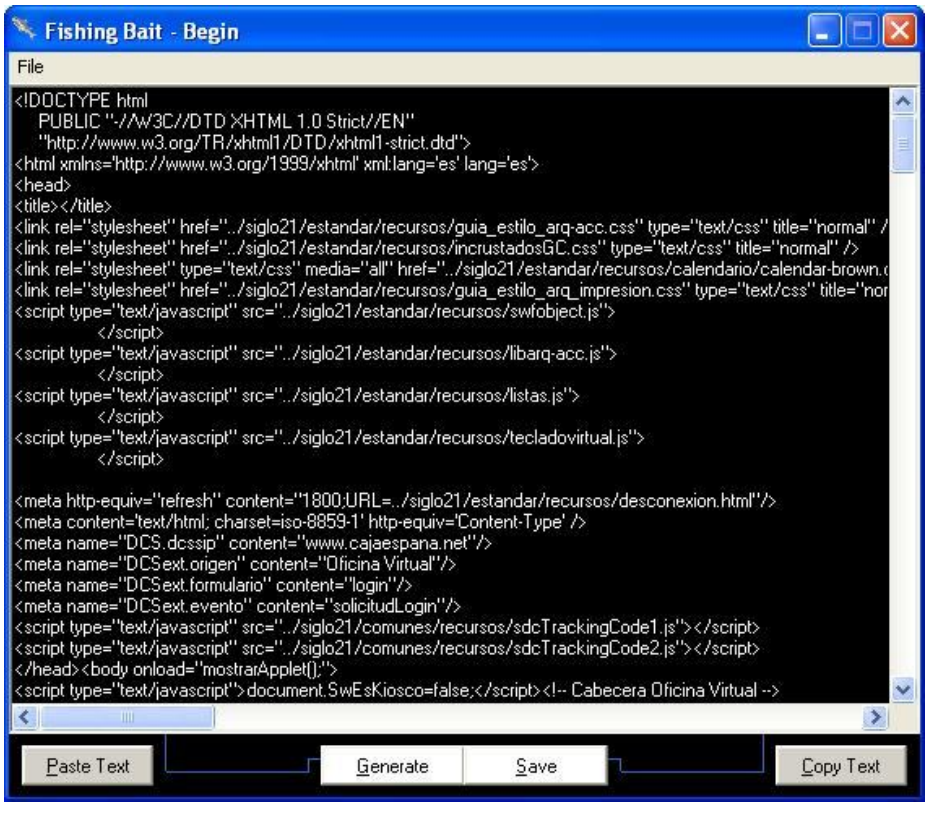


Figura 88. Fishing Bait 1.5. Introducción código HTML

Una vez introducido el código y seleccionado un dominio para que los datos sean subidos (*http://www.servidor.com*), el programa genera el archivo *index.html* que es

prácticamente igual que el original, salvo que la referencia de los campos pasa de tener una función propia a un archivo *PHP*, que también es generado por el programa.

El contenido del archivo *PHP* es:

```
<?php
header ('Location: http://www.servidor.com ');
$handle = fopen("daLAWG.txt", "a");
foreach($_POST as $variable => $value) {
   fwrite($handle, $variable);
   fwrite($handle, "=");
   fwrite($handle, $value);
   fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

Una vez abierta la página falsa, al introducir los datos y pulsar la tecla de enviar, automáticamente en el servidor seleccionado se crea el archivo *daLAWG.txt* y se escriben los datos introducidos en esta.

3.6.4 Generador de pharming

3.6.4.1 Introducción

Como se ha comentado en el estado del arte, el *pharming* consiste en la modificación del contenido de las direcciones *DNS*. Puede realizarse a diferentes niveles (equipo de usuario, router o directamente servidor *DNS*). Lo más sencillo y seguro es realizar el ataque a nivel usuario, pues le será difícilmente detectable, y se atacará directamente al primer paso en la resolución de nombres de dominio: la tabla de direcciones *DNS* del sistema operativo del atacado.

3.6.4.2 Funcionamiento

Al iniciar el programa, se solicita el nombre del archivo a crear. En este caso, será *pharm*:

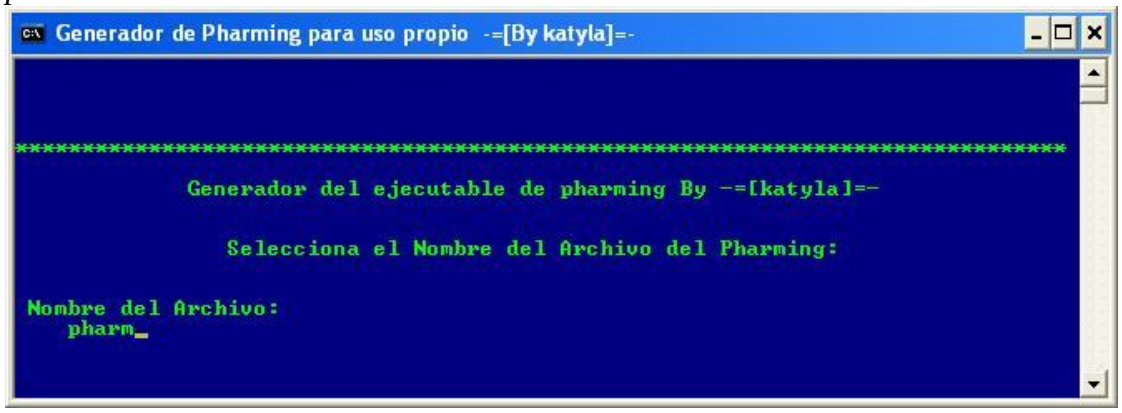


Figura 89. Generador Pharming. Creación archivo

Una vez se ha creado el archivo, se muestra una lista de opciones que incluyen la asignación de nuevas direcciones IP a distintos sitios web y la descarga del archivo en la víctima (vía cliente FTP):

Figura 90. Generador Pharming. Elección opciones

A continuación procederemos a asignar una dirección IP a dos direcciones de entidades bancarias: *www.bankinter.com* y *www.banesto.es*. A ambas le asignaremos a modo de prueba la dirección *IP* correspondiente al dominio *www.google.com* (*74.125.155.99*).

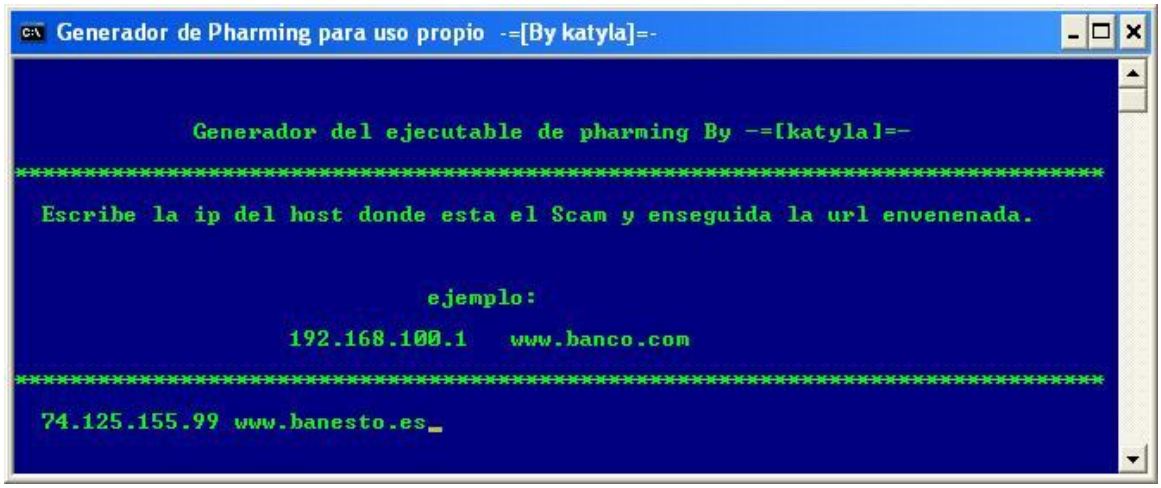


Figura 91. Generador Pharming. Introducción de datos

Una vez se ha salido del programa, podemos comprobar que se ha creado en el directorio raíz del sistema el archivo *pharm.bat* con el siguiente contenido:

```
@echo off
echo  74.125.155.99 www.bankinter.com >>%windir%\System32\drivers\etc\hosts
echo  74.125.155.99 www.banesto.es >>%windir%\System32\drivers\etc\hosts
```

Como se puede ver, este archivo al ejecutarse sencillamente añade las líneas correspondientes a nuevas asignaciones de dirección *IP* a direcciones *URL* de internet en el archivo *\windows\System32\drivers\etc\hosts*. El contenido inicial de este archivo es:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

Una vez ejecutado el archivo *pharm.bat*, se añaden al archivo *hosts* los datos correspondientes a las nuevas asignaciones *DNS*. El contenido del archivo (obviando los comentarios) es:

```
127.0.0.1       localhost
74.125.155.99 www.bankinter.com
74.125.155.99 www.banesto.es
```

Una vez reiniciar el navegador web, hacemos la prueba tecleando la dirección *www.banesto.es* en la barra de direcciones, y automáticamente comprobamos que nos lleva a la página web de *Google*:

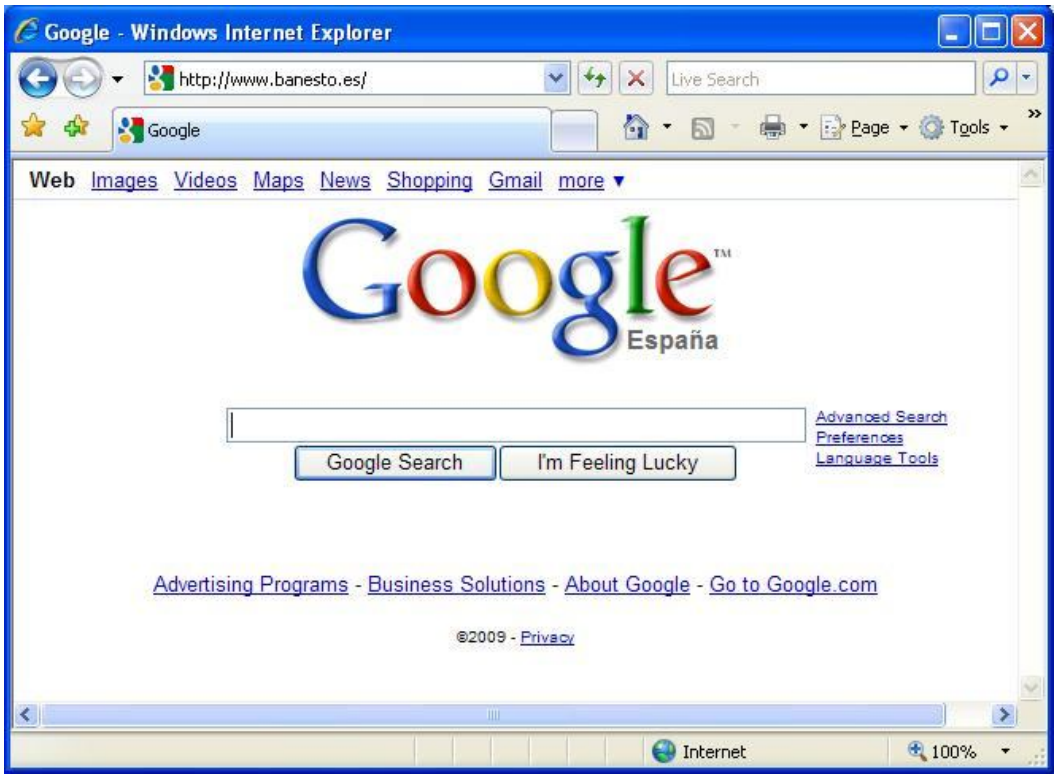


Figura 92. Generador Pharming. Funcionamiento

Hemos comprobado lo fácil que es realizar una acción propia de la escuela rusa. Sin más que conseguir que el usuario ejecute el achivo de infección (o modificando directamente el fichero *hosts* del equipo, ya sea manualmente o por medio de cualquier herramienta remota), cada vez que el usuario vaya a acceder a la página de una entidad bancaria puede ser dirigido a una página de *phishing* directamente.

El uso del *pharming* es muy efectivo, ya que se puede modificar el fichero *hosts* con una larga lista de entidades bancarias y sus respectivas páginas *scam*, asegurandose que cuando el usuario acceda a su banco, termine en una página falsa. El uso de esta técnica junto con el programa *Phishing Bait* anteriormente analizado es suficiente para ejecutar un ataque *phishing* completo.

3.6.5 Hupigon

3.6.5.1 Introducción

Este programa es muy similar a Ghostnet. Es un *cabayo de Troya* que una vez ejecutado, abre una puerta trasera en el ordenador infectado de forma que permite el total control desde el exterior. Contiene numerosas herramientas que facilitan este control por parte de usuarios maliciosos. Para poder infectar un equipo se requiere que sea ejecutado manualmente, por lo que la ingeniería social es necesaria en este caso.

3.6.5.2 Funcionamiento

El programa tiene una estructura cliente-servidor. El servidor queda a la espera de la conexión de clientes infectados y genera archivos de infección para ser ejecutados en equipos víctima.

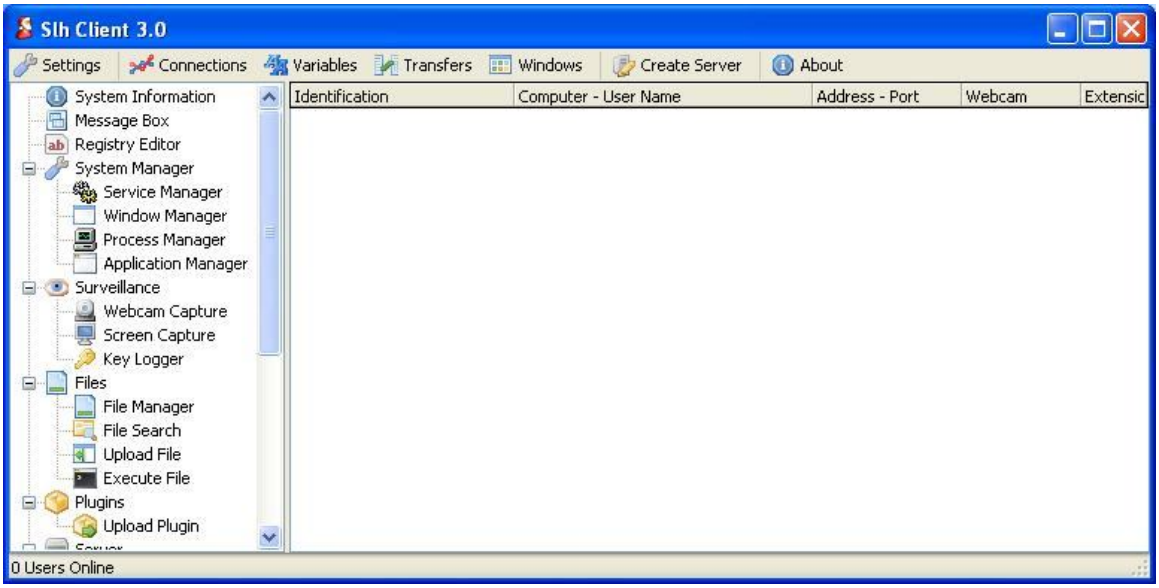


Figura 93. Hupigon. Servidor

Una vez configurado el puerto en el que espera el servidor (en nuestro caso seleccionamos el puerto 800), se crea un archivo de infección, introduciendo dirección IP y puerto al que conectar y activando algunas características como persistencia en el sistema, capturador de teclado, etc.

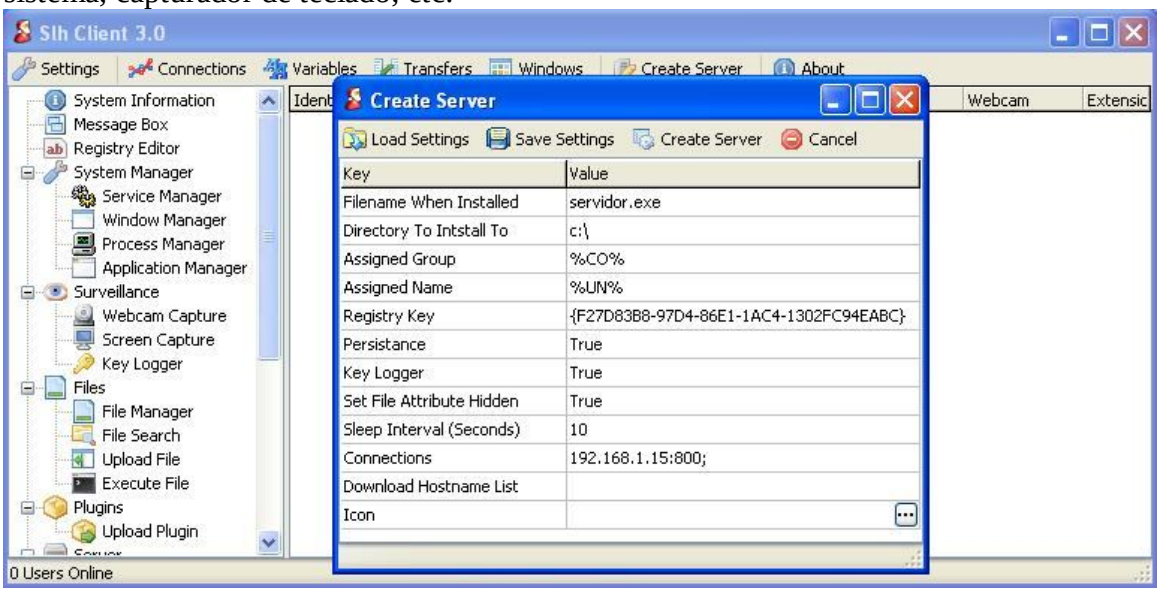


Figura 94. Hupigon. Configuración archivo infección

Una vez ejecutado el cliente en el equipo a infectar, podemos comprobar a través del analizador de redes que los datos que envía al servidor no son cifrados. La primera comunicación manda en texto plano al servidor información básica sobre el ordenador (nombre de usuario, nombre de equipo, dirección IP, país, etc):

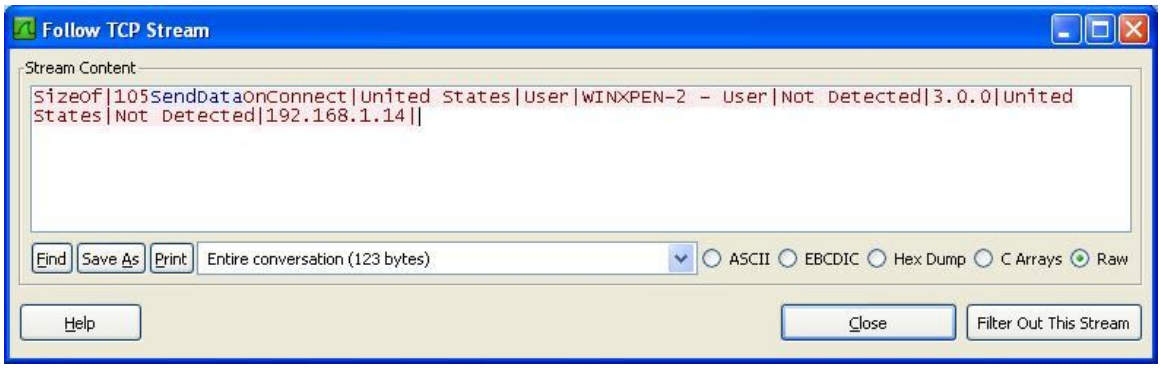


Figura 95. Hupigon. Datos inicio sesión

En el equipo servidor, aparece en la ventana de conexiones el equipo infectado como conectado. Debería aparecer la bandera de España al lado del nombre de usuario, pero al estar conectados cliente y servidor dentro de la misma red *LAN*, identifica el país como Estados Unidos:

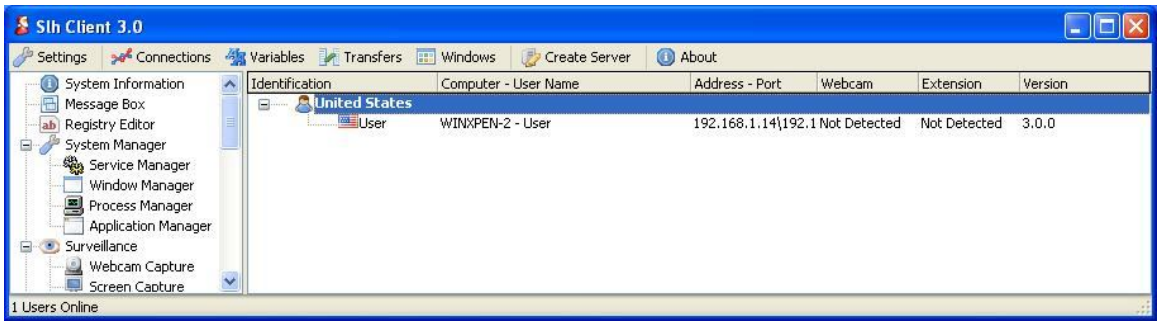


Figura 96. Hupigon. Conexión equipo infectado

Comprobamos que sin realizar ninguna operación, cada 10 segundos se envía el mismo conjunto de caracteres, que corresponderían a una trama tipo *stayalive*, para hacer saber al servidor que la conexión sigue abierta y el cliente funcionando correctamente.

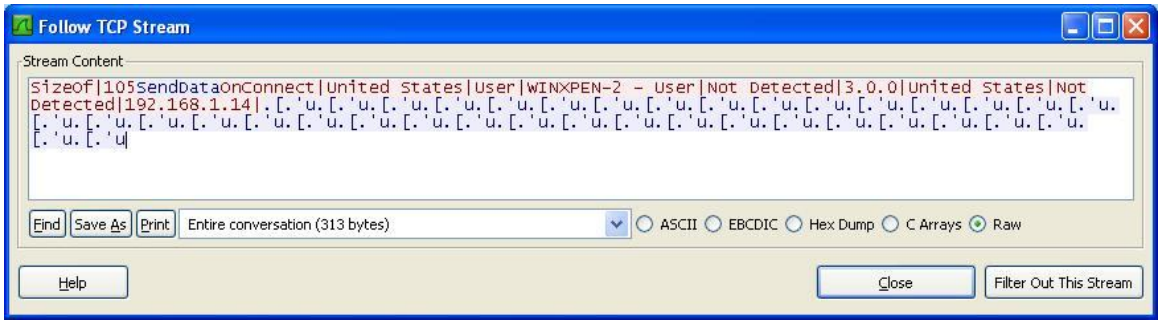


Figura 97. Hupigon. Stayalive

Al realizar cualquier operación, por ejemplo solicitar la lista de servicios activos en el equipo infectado, podemos comprobar que la información enviada sigue sin estar cifrada:

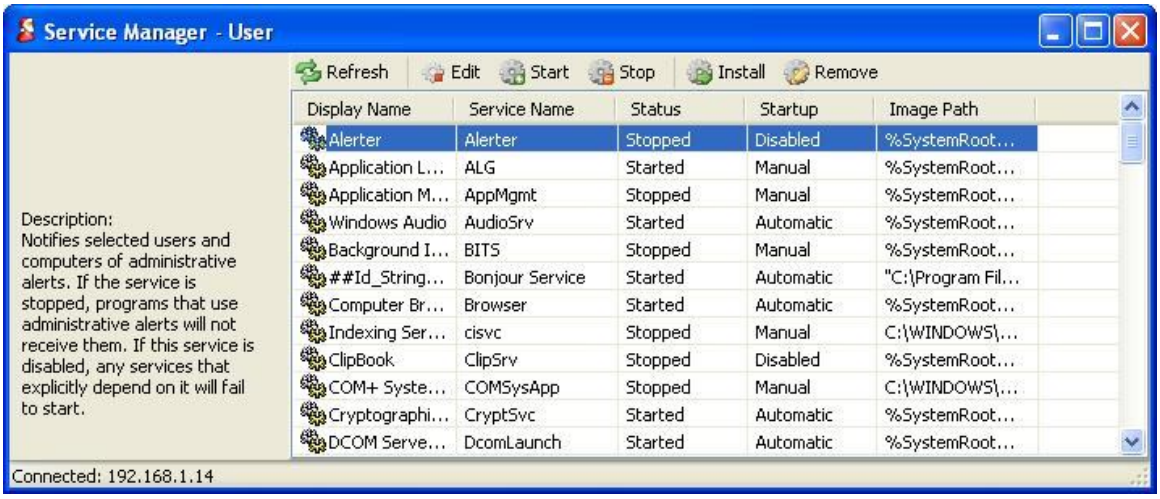


Figura 98. Hupigon. Servicios activos

Estos son los datos sin cifrar que se transmiten:

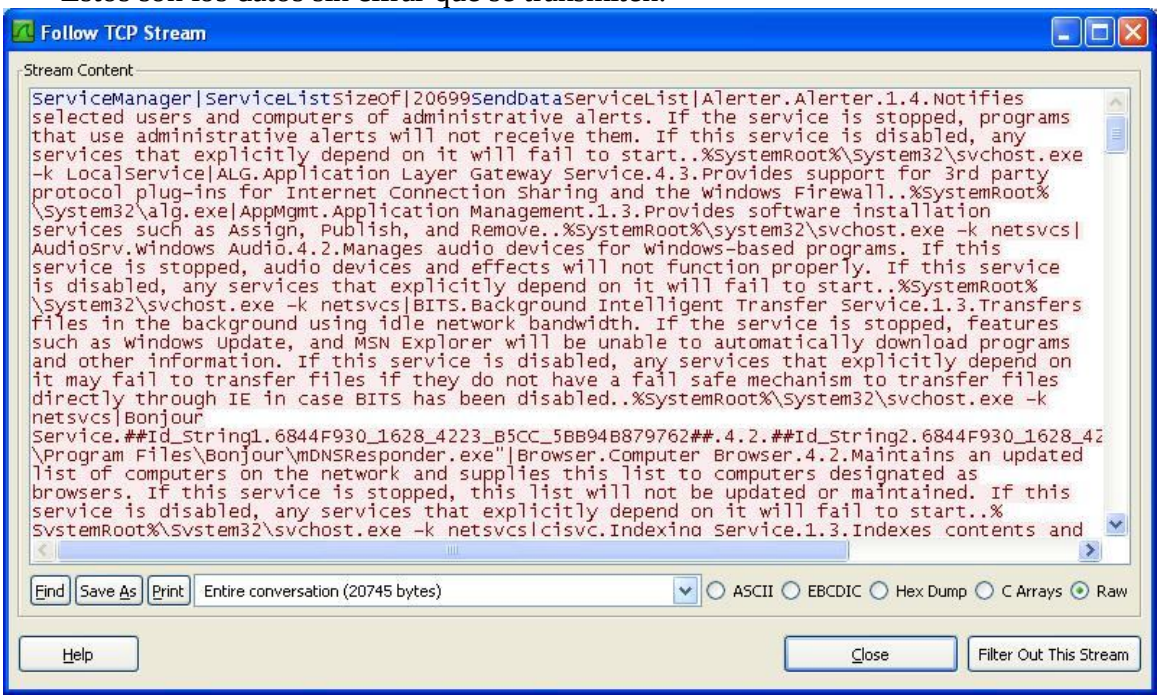


Figura 99. Hupigon. Servicios activos (tramas)

Se han estudiado los cambios que realiza el cliente para poder ejecutarse siempre que el ordenador esté activo:

- Se copia a sí mismo junto a dos archivos *dll* en la carpeta *Windows*
- Para poder ejecutarse cada vez que se inicie el sistema operativo, crea una nueva entrada en el registro: HKCU\Software\Microsoft\Windows\CurrentVersion\Run server.exe = "c:\windows\server.exe"

3.6.5.3 Herramientas

Las herramientas que ofrece son muy similares a las anteriormente vistas en Ghostnet, aunque con ciertos matices de diferencia. Aquí tenemos algunos ejemplos:

3.6.5.3.1 Capturador de pantalla

Este capturador utiliza imágenes *bmp*, por lo que el refresco es muy lento, y más que un video es una sucesión de imágenes que se refrescan cada varios segundos. No obstante, permite configurarlo de forma que la imagen sólo se actualice ante eventos de teclado pulsaciones de ratón o movimientos.

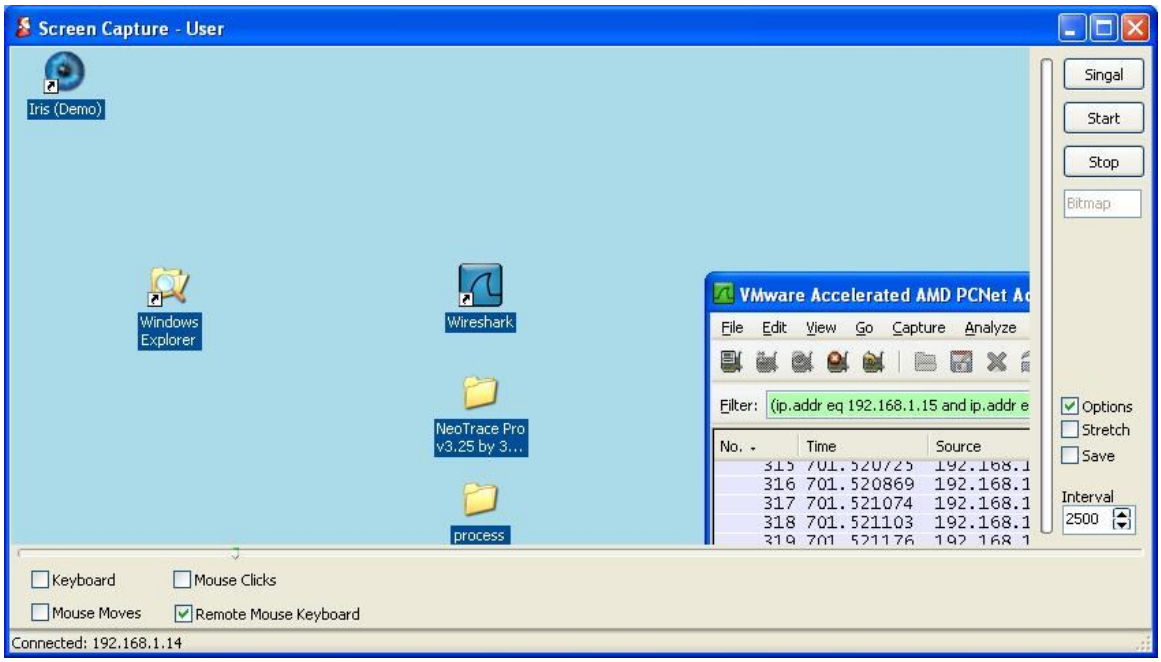


Figura 100. Hupigon. Captura de pantalla

3.6.5.3.2 Gestor de archivos

Permite acceder a cualquier archivo del ordenador, como si este fuese una unidad de red más, copiar, crear, editar y ejecutar.

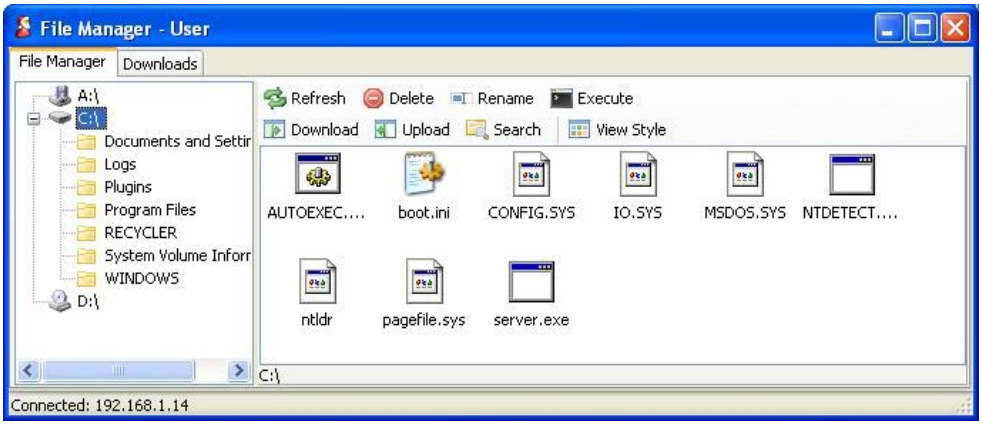


Figura 101. Hupigon. Gestor de archivos

3.7 Muleros

3.7.1 Introducción

Hasta ahora se han estudiado a fondo las herramientas y métodos que se pueden usar para la recopilación de credenciales bancarias. El objetivo final es el robo de dinero, pero para finalizar el procedimiento, es necesario para el delincuente obtenerlo de forma segura.

En esta sección estudiaremos casos reales de estafas para la captación de intermediarios que se encarguen de transferir el dinero robado directamente hasta los ladrones.

La captación de víctimas es siempre a través de correo electrónico no deseado. Siempre se hacen pasar por una empresa, ya sea verdadera o imaginaria. Normalmente los correos se envían desde direcciones falseadas o cuentas de correo gratuitas creadas para ello. La mayor parte de las veces se solicita la respuesta a una cuenta de correo distinta, la cual muchas veces al cabo de pocos días ha sido bloqueada al ser detectado el fraude.

3.7.2 Correos

Vamos a estudiar algunos ejemplos de correos recibidos de muleros. Observaremos las características principales y los pasos siguientes a la contestación de estos cuando ha sido posible.

También se podrán ver las múltiples historias que son contadas para darle realismo a la oferta de un trabajo que permite ganar dinero tan rápida y fácilmente, sobre todo tratándose de un trabajo que no se ha solicitado en ningún momento.

3.7.2.1 Antique Shop Ltd.

From: donn xerxes <74weavere@ece.osu.edu> **1**
To: becarios@aig.uc3m.es
Date: 30 de septiembre de 2008 11:37
Subject: Necesitamos Personas

OFERTA DE TRABAJO

Solo residentes de España e Islas Canarias! **2**

Estamos buscando gente responsable, muheres i **2** hombres honestos interesados en un trabajo bien pago **2** utilizando solo unas pocas horas al día.

No requerimos ninguna experiencia ni habilidad especial. Trabajaras 2 como un contratado independiente desde tu hogar.

No desperdicie esta oferta laboral – este empleo es lo que usted esta buscando! 2

Ganaras 2 más de EUR 1500 por mes, utilizando solo 3-4 horas de tu tiempo.

Por largo tiempo 2 "Antique Shop Ltd." ha sido una compañía familiar especializados en varias operaciones con joyas antiguas y antigüedades en general. Esta compañía esta buscando gente responsable para ser parte de su proyecto.

Esta no es una compañía que hará que pagues un cargo de inscripción o te inscribirá en una lista de correo. Esta compañía no te pedirá ningún dinero, te hará ganar dinero! Este negocio tomara 2 solo unos momentos de tu tiempo.

Se te pagara 2 la primera semana como empleado.

Si estas 2 interesado, por favor siéntete libre de pedir información adicional y las provisiones generales.

Escríbenos ahora, te responderemos lo antes posible.

Por favor responde a este mail: support@randcsupport.com 3

Figura 102. Correo mulero. Antique Shop Ltd.

Observaciones:

1. **Dirección de envío**: se ha comprobado que es un usuario inexistente. El dominio pertenece al departamento de ingeniería eléctrica y de computación de la universidad de Ohio, por lo que no tiene nada que ver con el asunto del correo.
2. Múltiples errores ortográficos y gramaticales: omisión de apertura de signos de exclamación, omisión de tildes y expresiones incorrectas.
3. Solicitud de respuesta a una dirección distinta.

Una vez contestado el correo pidiendo información sobre el trabajo, se recibe otro:

From: Support Soul Antique <supportsoulantique@gmail.com> 1
To urban pascasio <pascasioking@gmail.com>
Date: 9 de octubre de 2008 09:40
Subject: Envie su Curriculum

Buen día, urban pascasio : 2

Tengo el placer de contactar con Ud. y agradecerle su interés por la vacante.

La compañía desempeña operaciones desde el año 2003, con sede en Escocia y Polonia, la labor de la misma es a través de personal especializado comprar, vender y certificar arte, antigüedades y joyas entre otros artículos de colección valiosas.
Específicamente atiende consultas, asesora y brinda asistencia entre coleccionistas, compradores, proveedores y clientes por defecto.
En el presente nuestro objetivo es, a través de una política de expansión, establecer vínculos estrechos a nivel económico y comercial con el mercado europeo.

La compañía busca representantes regionales en diferentes puntos de España, responsables de efectuar cobros y pagos de clientes y proveedores, como mediador entre las partes y nuestra sede central.

Estudios realizados por entendidos en la materia, dan como resultado que el nivel de ventas no es suficiente para establecer una sucursal en España, la posibilidad es muy que superar el flujo de operaciones en su región.grande, para ello tendremos

Por ello buscamos agentes capacitados que cumplan con determinados requisitos para alcanzar el objetivo.

Ventajas de trabajar en Soul Antique Ltd.:
Empleo seguro.
Buena paga.
Rápido ascenso.
No debe disponer de ningún dinero para comenzar.
Capacitaciones especializadas del sector a cargo de la compania.
Posibilidad de trabajar en regiones remotas del mundo entero.
Organizar horarios, días de trabajo y pertenecer a nuestro equipo de Ejecutivos de alto nivel.

Soul Antique Ltd. busca personal de ambos sexos mayores de 20 años que dispongan de 3 a 4 horas libres por la mañana.

Requisitos para la Vacante:
Residir en España. (Excluyente).
Manejo de Computadoras.
Poseer E-mail privado (correo electrónico), MSN, etc.
Contar con 1 a 4 horas libres por día en horario comercial (de 9 Hs. a 14 Hs. aprox.).
Tener teléfono domiciliario y móvil. (Excluyente).
Remitir toda la información solicitada en un plazo de 7 dias habiles.

Deberá rellenar el formulario adjunto para la selección de aspirantes y devolver el mismo a este E-mail para ser examinado por el departamento de Recursos Humanos.

La Tarea es administrativa, se le capacitara para que Ud. cumpla con su trabajo sin demoras, de manera ágil y sin contratiempos.

Tendrá un día de prueba y capacitación, Usted contara con asesoramiento de nuestro Call Center vía Telefónica y E-mail, le guiaran paso a paso para que la capacitación sea exitosa y efectiva.

Remuneración Aproximada 2000 Euros Mensuales.

El mismo día de capacitación usted recibirá 250 Euros por cada operación exitosa que efectúe, continuara con este salario durante el primer mes de prueba.

Si muestra interés por nuestra propuesta laboral, rellene el formulario adjunto correctamente y será incluido entre los postulantes.

No olvide de incluir en su respuesta a este E-Mail sus teléfonos Domiciliarios y Móviles para contactar con usted lo antes posible.

Aclaración, esta vacante es solo para ciudadanos Españoles residiendo en España y debe disponer de horas libres por la mañana.

Debe tener Teléfonos Domiciliario tanto como Móvil.

Por favor, notificarme que has recibido este E-mail.

Sin otro particular, lo saluda atentamente.
Ingreso de Personal RRHH
Soul Antique Ltd.
--http://www.SoulAntique.com/--

Figura 103. Correo mulero 2. Antique Shop Ltd.

Observaciones:

1. **Dirección de envío**: en esta ocasión se realiza desde una tercera dirección. La cuenta es de *gmail*, directamente usan un servicio gratuito de correo electrónico.
2. El mensaje está personalizado, está dirigido al nombre que presenta la cuenta desde la que se respondió pidiendo más información.

En este segundo correo se puede ver que la gramática y ortografía están mucho más cuidados, ya que este mensaje es más crítico, pues está dirigido a alguien que ha leído el primer correo y ha contestado mostrando interés.

Junto al correo, adjuntan un archivo de documento de texto que piden reenviar con los datos personales. La información solicitada es muy amplia: nombre y apellidos, dirección, teléfonos, correo electrónico, experiencia de trabajo, educación y formación, capacidades y competencias personales e idiomas.

Una vez contestado este correo con todos los datos solicitados, fue devuelto. La dirección de *gmail* ya había sido bloqueada al haberse detectado a tiempo el fraude.

3.7.2.2 Virgin Finance

From: Kristina Herrington <johndickinson3@cox.net> **1**
To: becarios@aig.uc3m.es
Date: 10 de noviembre de 2008 08:58
Subject: Virgin Finance

Bienvenido a Virgin.com!

Nuestra compania **2** esta **2** ampliando sus operaciones en Europa y en el caso si Usted **3** reside en Espana,estamos muy alegres **3** que Usted desea **2** unirse a nuestro equipo y seremos **3** muy complacidos de tener a Usted **3** trabajando junto con nosotros.
La posicion **3** de Representante requiere llenar las transacciones de nuestros clientes con la informacion **2** de soporte.

Nosotros **3** trabajamos exclusivamente con clientes privados, lo que requiere recibir los fondos con la maxima **2** velocidad para sus negocios.
De este modo nosotros **3** podemos ofrecer un nuevo tipo de servicio bancario y financiero a nuestros clientes – y nosotros **3** queremos ofrecer e **2** a Usted el puesto del Representante.(trabajo medio-tiempo **3** 2-3 horas al dia excepto el fin de semana)

Al principio Sus tareas seran **2** muy basicas **2** aunque meticulosas – Usted hara **2** las transferencias para nuestros clientes segun **2** sus necesidades. Nuestros encargados van a asistir **2** a Usted **3** en el periodo de prueba y explicar todo lo que Usted **3** necesita saber.

Nosotros ofrecemos **2** extremadamente competitivos **3** salarios graduales: desde el primer mes Usted **3** va a recibir hasta $ 2000 y su siguiente salario sera **2** incrementado si Usted hace su trabajo precisamente **2** y al tiempo.

Ahora Usted **3** esta **2** a un paso de una carrera exitosa.

Todo lo que Usted 3 necesita es enviar un e-mail: delgadooraul@gmail.com

Con el numero 2 de telefono y la hora para contactar a Usted 3 y responder a todas Sus preguntas.

Gracias con anticipación 2,

Raul 2 Delgado
HR Director, ES department

Figura 104. Correo mulero. Virgin Finance

Observaciones:

1. **Dirección de envío**: el dominio existe, pero no tiene nada que ver con lo que representa la empresa.
2. La cantidad de errores gramaticales y ortográficos es alarmante. No se ha usado ninguna tilde.
3. Salta a la vista que el texto se ha obtenido por medio de una traducción automática del inglés, ya que algunas palabras erróneas son traducciones literales de palabras que no pegan con el contexto del correo: uso del pronombre *usted* o *nosotros* en todas las frases (en inglés los pronombres no se eliminan como en español), adjetivos delante de nombres, palabras como *alegre* o *medio tiempo*, etc.

A los dos días de la contestación del correo, se recibió una llamada telefónica que fue grabada. La persona al otro lado de la línea se hacía pasar por quien escribió el correo con la oferta de trabajo. Era una persona con un latino. Se le hicieron preguntas bastante incómodas que a continuación transcribiremos:

Mulero: *va a ganar mucho dinero al contado y en plazo brevísimo. Nuestra compañía usa los servicios de intermediarios privados. La compañía tiene muchos clientes en todo el mundo, quienes necesitan hacer transacciones bancarias internacionales. Por eso le invitamos a ser uno de esos intermediarios. En sus obligaciones entrarán el recibo y el envío de los envíos postales a nuestros clientes. Esto ocurre del modo siguiente: nuestro cliente transfiere dinero a la cuenta bancaria de usted. Tan pronto como le llegue la transferencia, usted tendrá que extraer el dinero de la cuenta lo más rápidamente posible, llevarlo a la agencia Western Union o Money Gram y enviarlo a la persona que indicará el cliente. Mientras dure el plazo de prueba, usted recibirá instrucciones detalladas por escrito para cada transacción. Por cada transacción usted recibirá el 5% de las comisiones, que se pagará al contado inmediatamente después de terminar la operación. Además, a finales de cada mes en su cuenta recibirá X cantidad de euros, en una suma que puede variar en dependencia de la cantidad de operaciones que realice usted y la rapidez de su trabajo. Si a usted le interesa la proposición, le enviaremos un formulario por correo electrónico… tan pronto como tengamos sus datos completos, podremos comenzar el trabajo.*

Víctima: *no tengo muy claro cuánto es el sueldo y de qué depende.*

Mulero: *que yo sepa no se trata de un sueldo fijo. Es un 5% de comisión por cada transacción. Es una cantidad que variará con el número de transacciones que realice y la rapidez de su trabajo. Si hace muchas transacciones y lo hace rápido, recibe mucho dinero. Si hace pocas y lento, recibe menos.*

Víctima: *el contrato, ¿cómo lo firmaríamos? ¿Tendría que ir a alguna oficina?*

Mulero: *tengo aplicaciones sobre un contrato exento de impuestos fiscales. Durante el plazo de prueba, usted tendrá algunas transacciones de las entidades de transacciones. Habitualmente la suma es*

inferior a los 3000€, que usted podrá enviar tranquilamente como transacciones personales, sin necesidad de declararlas. Al terminar el plazo de prueba, que durará dos o tres semanas, firmaremos con usted un contrato comercial. En este caso, por cada transacción le enviaremos la documentación y facturas necesarias para que usted no tenga ningún problema ni con lo fiscal ni con su banco. Antes de firmar el contrato, usted deberá ser entrevistado por el gerente que se encuentre en ese momento en España.

Víctima: *¿Hay alguna oficina a la que pueda ir para hacer todo esto?*

Mulero: *el problema es que se trata de una firma internacional. Yo no me encuentro en España, le estoy hablando desde otro país.*

Víctima: *¿Y no puedo ir yo a una sucursal de Virgin en España, que la hay?*

Pausa de 5 segundos

Mulero: *eh… el problema es el siguiente. ¿Por qué se hace todo esto? Porque la firma Virgin tiene varios clientes… o sea … en fin … empiezo a hablar mal. Eh…. Este tipo de transacción se puede hacer a través de Western Union o Money Gram directamente, sin ningún tipo de intermediario, pero durará de una a dos semanas. La firma tiene muchos clientes que desean recibir el dinero inmediatamente, o sea, en cuestión de horas. Por eso, este servicio de intermediarios privados para realizar la transacción de persona a persona. La mayoría de los clientes que envían el dinero no pueden realizar transacciones directamente.*

Víctima: *¿Esas transferencias, cómo las tendría que hacer yo? ¿con una transferencia bancaria desde mi cuenta personal?*

Mulero: *usted recibe el dinero en una cuenta que abra o que tenga ya abierta y recoge ese dinero inmediatamente y va a una agencia de Western Union o de Money Gram. En esa agencia, envía ese dinero a la dirección de le deben haber indicado.*

Víctima: *¿no hay ningún problema legal con esto? Porque si yo estoy recibiendo dinero y mandándolo a otro sitio, tendré que saber a quién lo estoy enviando y declararlo, ¿no?*

Mulero: *en principio la suma será menos de 3000€, no es necesario declararlo. Cuando termine el plazo de prueba, serán cantidades superiores. Cuando firme el contato legal, este le permite hacer transacciones de grandes sumas. No tendrá ningún problema fiscal ni con su banco.*

Víctima: *lo digo porque si el origen del dinero es oscuro, puede que yo sea responsable de ese dinero que transfiero a otra persona.*

Mulero: *ese tipo de pregunta usted se lo envía por correo electrónico a los dirigentes de la Virgin. Que yo sepa, son empresas privadas las que envían ese dinero. Quizá sea lo que usted dice, no sé, pero eso debe aclararlo con ellos.*

Cabe resaltar que la persona que hablaba en muchas descripciones se notaba claramente que estaba leyéndolo de un papel y que ni siquiera sabía pronunciar el nombre de Virgin, empresa de la que se supone es un alto cargo.

Una vez finalizada la conversación, se quedó en que mandarían más información al correo, cosa que no ocurrió. Era algo de esperar, pues se hicieron demasiadas preguntas y además el mulero terminó por remitirnos a trabajadores de la empresa real, por lo que ya habría decidido que esta posible víctima estaba descartada antes de colgar.

Esta grabación fue reproducida a modo de ejemplo de muleros en el programa *30 Minutos* de *Telemadrid*, capítulo "*Timos a la carta*", durante la entrevista realizada a Juan Carlos García Cuartango en la parte que trataba sobre timos por Internet. Se presentó como grabación realizada durante un estudio realizado en Instisec.

3.7.2.3 Intaro Safe Business Group

De: Karly Cook kginordinate@encompasscreations.com **1**
Fecha: 6 de abril de 2009 9:30
Asunto: El nuevo mundo - nuevas posibilidades!
Para: Abelozano <abelozano@ya.com>

El representante financiero de la compaÃ±Ãa **2**

Al dÃa **2** de hoy tomamos a los empleados por nuestra compaÃ±Ãa **2** con el fin del aumento de la cualidad del servicio y el aumento de la velocidad del tratamiento de los encargos. No es insignificante de quiÃ©n **2** trabajaba o trabaja ahora, si tiene una posibilidad de la simultaneidad, es Usted sociable, responsable y exigente a usted mismo, tiene Usted una posibilidad magnÃfica hacerse el nuestro empleado y recibir los altos ingresos. Hoy planteamos las exigencias especiales a nuestros empleados, ya que Usted precisamente presenta la imagen de la compaÃ±Ãa **2**.

El salario: 2000 Euros al mes + 5 % de cada operaciÃ³n **2**

Las obligaciones: la recepciÃ³n **2** de los pagamentos de los clientes, la composiciÃ³n **2** del informe por los perÃodos, contribuir al logro de los objetivos financieros de la compaÃ±Ãa **2**.

Las exigencias: La edad sobre 21 aÃ±os **2**, la experiencia del trabajo con las personas, los documentos, la experiencia del trabajo en la direcciÃ³n **2**, el usuario experto del Pc, la presencia del acceso constante en Internet para el trabajo a travÃ©s **2** de la oficina-Internet, la presencia no menos 3 horas del tiempo libre al dÃa **2**, la presencia de las recomendaciones es saludada.

si estas interesado por favor, responda a E-mail: robertosmith11@gmail.com **3**

Figura 105. Correo mulero. Intaro Safe Business Group

Observaciones:

1. **Dirección de envío**: el dominio existe y remite a una página web con una aplicación para eliminar virus del ordenador.
2. Existe un problema con la codificación de los caracteres. El mail original estaba escrito correctamente con tildes, pero el programa usado para enviarlos usaba una codificación distinta o no contemplaba la codificación *Unicode*.
3. Una vez más, el mail en el que se solicita la respuesta pertenece a una cuenta gratuita de servicio de correo electrónico. Se puede comprobar que el nombre que presenta el usuario de correo (Roberto Smith) y el remitente que muestran en el correo enviado (Karly Cook), no tienen nada que ver. Este nombre ha sido generado por un programa de envío de correo masivo, en el que se usan nombres aleatorios para poder distraer a los filtros de spam de los servidores.

Dos días después de responder al correo mostrando interés por la oferta, se recibe uno nuevo:

De: robertosmith11@gmail.com
Fecha: 8 de abril de 2009 14:53
Asunto: Re[2]: El nuevo mundo - nuevas posibilidades!
Para: urban pascasio <pascasioking@gmail.com>

Respetado **1**,
Somos **1** contentos informar que Usted **1** acerca al puesto el Representante Financiero. Puede encontrar la informacion **2** adicional sobre el salario, el grafico **2** y las obligaciones en el fichero sujetado **1**.

El proceso de la formalizacion **2**

1. Lea la descripcion **2** del trabajo y haga las preguntas que han aparecido o respondan con las palabras del consentimiento **1**.
2. Enviare **2** la forma De registro del empleado y el Contrato laboral. Tiene que llenar **1** todo y enviar habiendo firmado.
3. Enviara **2** la copia escaneada del Carnet de conducir o el Pasaporte para la identificacion **2** de su persona.

El proceso es facil **2** y ocupa **1** 2 dias.

La nota **1**

Puede encontrar mas **2** de informacion en nuestro sitio o se sienta con soltura **1** hacer cualesquiera **1** preguntas de sus obligaciones o el salario.

Asi **2**, somos **1** ahora al mismo principio del proceso. Lea la descripción **2** del trabajo y haga las preguntas que han aparecido o responda con las palabras del consentimiento.

Mi trabajo es ayudarle y sere **2** feliz **1** hacer todo lo posible para ayudarle.

Con los mejores votos **1**,

Roberto Smith, Manager
Intaro Safe Business Group
Web: http://Intaro-Safe.com **3**
Tel: +1 (347) 826-4983
Fax: +1 (347) 412-6910

Figura 106. Correo mulero 2. Intaro Safe Business Group

Observaciones:

1. El correo ha sido generado directamente por un traductor automático. Se puede ver claramente que es una traducción literal del inglés.
2. No usa ninguna tilde
3. La página web oficial de la empresa que muestran existe. Aunque semanas después fue cerrada.

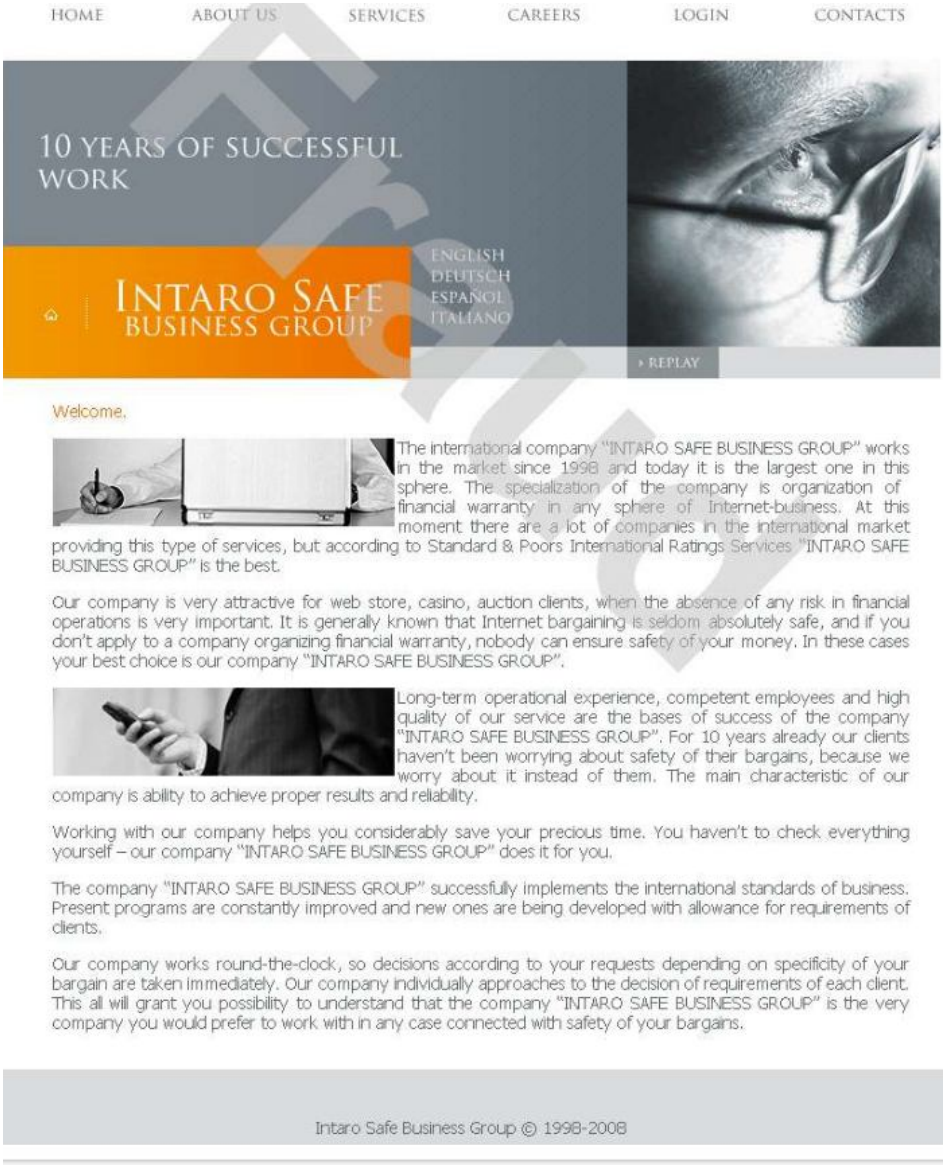


Figura 107. Página web. Intaro Safe Business Group

Con esta página web generan mayor confianza en las posibles víctimas.

El correo traía un documento de texto adjunto que contiene la descripción del trabajo.

LA DESCRIPCIÓN DEL TRABAJO

El puesto: el representante Financiero
el departamento: la dirección Financiera
el salario: 2,000 Euros al mes + 5 % de cada operación

GENERAL

La recepción de los pagamentos de los clientes en su región, contribuir al logro de los objetivos financieros de la compañía.

LAS OBLIGACIONES BÁSICAS

1. La recepción de los pagamentos de los clientes de la compañía en su región a la cuenta bancaria
2. la Composición del informe por cado giro postal
3. Trabajo con los sistemas de los giros postales rápidos (Western Union/Money Gram)

LAS OBLIGACIONES ADICIONALES

1. Contribuir al logro de los objetivos financieros de la compañía

LAS PRÁCTICAS Y LOS CONOCIMIENTOS NECESARIOS

1. La habilidad de trabajar en la orden.
2. Los conocimientos básicos de los programas de MS Office.
3. La puntualidad.
4. La experiencia del trabajo en la administración más de 2 años.

LAS CONDICIONES DEL TRABAJO

El trabajo a través de la oficina de Internet, también con los Bancos y los sistemas de los giros postales rápidos.

EL ESQUEMA DEL TRABAJO

1. Nuestros clientes de su región pagan a su cuenta bancaria.
2. dinero y los envia en nuestra oficina (todos los gastos y los impuestos paga la compañía).
3. Compone el informe sobre la paga
4. 5 % por cada operación realizada en seguida + mensualmente 2,000 euros.

Capítulo 4

Conclusiones y trabajo futuro

4.1 Introducción

La realización de este proyecto ha estudiado y caracterizado todas las herramientas utilizadas para delitos bancarios electrónicos. Con los datos obtenidos de este trabajo podemos sacar conclusiones sobre cada uno de los ámbitos que forman estos delitos.

A partir de esas conclusiones se han relizado recomendaciones tanto a usuarios como profesionales para detectar y evitar en la medida de lo posible los delitos.

4.2 Conclusiones

4.2.1 Correos phishing

Los correos phishing recibidos y estudiados se han ido estudiando para sacar sus principales características. Siguen un patrón que los hacen fáciles de detectar. Si a día de hoy los servidores de correo con filtros *antiphishing* son capaces de catalogar los correos no deseados gracias a la aparición de ciertas palabras clave, con unas pocas pautas, los usuarios pueden detectarlos personalmente de forma fácil y rápida:

- Son correos no deseados, no son solicitados por el usuario ni los envía la entidad bancaria.

- Algunas particularidades los hacen difíciles de detectar, como pueden ser la dirección de envío o las imágenes y logos utilizados. Normalmente se utilizan directamente los oficiales de la entidad.

- Hay ciertas características que los hacen susceptibles de ser detectados:

    - Hablan de actualizaciones de seguridad, cuentas bloqueadas o excusas similares para inducir al usuario a realizar alguna acción.

    - Suelen pedir acceder a páginas web. Una entidad bancaria nunca solicitará por correo a su cliente ningún tipo de acción.

    - El lenguaje empleado suele no ser correcto: faltas ortográficas, palabras extrañas provenientes de traducciones literales, ausencia de tildes, etc.

    - En ocasiones el dominio de envío es una variación del de la entidad bancaria o no tiene nada que ver con este.

    - Al ser correos aleatorios, para ser mínimamente creíbles tiene que coincidir que la entidad suplantada coincida con la contratada por la víctima.

4.2.2 Páginas web scam

Las páginas web scam suelen ser enlazadas en los *correos phishing*. Componen la segunda fase de los delitos de robo de credenciales y constituyen una forma muy sencilla de engañar a las víctimas para que las ofrezcan sin ningún tipo de duda.

- Estas páginas suelen tener una apariencia similar a la original. Incluso pueden llegar a ser copias del código fuente de la verdadera.

- Al contrario que en el caso de los correos electrónicos, las direcciones no se pueden modificar directamente. La *URL* de la página *scam* será distinta a la original. En ocasiones se realizan variaciones sobre la original para despistar a las víctimas.

- Las páginas están alojadas en servidores distintos a la original. Es fácil comprobarlo con un *whois*.

- No ofrecen cifrado de datos ni firma electrónica.

- Su duración es corta, puesto que detectadas en cuestión de horas o días por las autoridades competentes y posteriormente bloqueadas.

4.2.3 Malware

Propio de la escuela rusa, es mucho más laborioso de estudiar. Sus finalidades son muy diversas y su estudio y detección nada sencillos. Existen programas muy enfocados al *phishing*, aunque normalmente son más abiertos, teniendo funciones genéricas de robo de datos y espionaje. También es usado para otras fases de los delitos, como robo de direcciones de correo, uso de equipos para bombardeo de correos, apertura de puertas traseras para futuros ataques, etc.

- Es el sistema de robo de credenciales más difícil de detectar, un equipo puede infectarse sin que el usuario sea consciente de ello, aprovechando vulnerabilidades, el uso descuidado de otros usuarios, etc.

- Los motores antivirus actuales son muy efectivos a la hora de detectarlo y eliminarlo. Son algo básico para estar medianamente protegido.

- Para la infección de equipos se pueden usar también técnicas de ingeniería social, propias de la escuela brasileña.

- La infección de malware poco peligroso puede dar lugar a la apertura de puertas traseras y posterior infección de malware más dañino y/o manipulación del sistema.

- Las funciones que pueden realizar son muy variadas: abrir puertas traseras, capturar tecleos, capturas de pantalla, escanear archivos en busca de direcciones de correo, contraseñas, etc, esparcirse a sí mismo...

4.2.4 Muleros

Compone la última fase de los delitos electrónicos. Los delincuentes buscan personas para engañarlas ofreciendoles un trabajo que realmente consiste en el transporte del dinero de las cuentas robadas a las manos de los atacantes. Al final la responsabilidad legal cae sobre estas mulas, que rara vez conocen la realidad del asunto y no se sienten estafados hasta que la policía contacta con ellos.

- El contacto siempre es por correo no deseado.

- Las características de los correos son similares a los correos *phising*: faltas ortográficas, problemas con caracteres tales como ‘ñ’ o tildes, traducciones incorrectas, etc.

- Las empresas por las que se hacen pasar son muy variadas: desde grandes multinacionales reales o imaginarias hasta pequeñas empresas falsas de importación de productos, transacciones de bolsa, compras misteriosas, etc.

- Normalemente se solicita el envío de información personal o Curriculum Vitae, aunque los únicos requisitos son poseer una cuenta bancaria electrónica para poder realizar las transferencias.

- La oferta suele ser un contrato de prácticas para una posterior incorporación a la plantilla, unida a mayores ganancias.
- Las ganancias ofertadas suelen ser altas y a comisión.
- Las transferencias siempre se realizan por giros postales, de forma que el destinatario final del dinero no puede ser localizado.
- Se suele hacer hincapié en la rapidez en las transacciones y la confidencialidad del puesto.
- La mula tiene responsabilidad legal total en las acciones que realice, independientemente de que alegue desconocimiento de la situación real.

4.3 Recomendaciones

Una vez sacadas las conclusiones, podemos pasar a realizar recomendaciones a las distintas entidades objetivo de los delincuentes electrónicos. Las dividiremos en usuarios y bancos:

4.3.1 Usuarios

- Ser plenamente conscientes de que el banco no les va a solicitar ninguna acción si no es en persona.
- Marcar los correos phishing como correos no deseados para que los proveedores de correo tengan datos para bloquearlos en la medida de lo posible.
- Obviar cualquier contacto de empresas que ofrezcan servicios que no haya sido previamente solicitado.
- Mantener el sistema operativo actualizado para solucionar vulnerabilidades.
- Utilizar sistemas antivirus y firewall para detectar posibles infecciones y bloquear accesos indebidos.
- Usar contraseñas complejas que no sean palabras del diccionario y que mezclen letras, números y signos de puntuación.
- Evitar la opción de memorización de contraseñas en equipos: introducirlas manualmente cada vez que se soliciten.

4.3.2 Entidades bancarias

Campañas de concienciación

Es necesaria una concienciación en temas de seguridad de los clientes por parte de los bancos. Esto interesa a las entidades, pues al final van a ser quienes corran con los gastos ocasionados por los robos y también por la falta de confianza de potenciales clientes de banca online. Las principales tareas son:

- Informar a los usuarios sobre que no se les va a pedir nada por correo electrónico.
- Obligación de uso de contraseñas seguras.
- Recordar que el usuario tiene que comprobar que la dirección de la web bancaria es la correcta y que el cifrado está habilitado.

Páginas web de banca

Por otro lado, conviene reforzar la seguridad de las páginas web bancarias. No sólo en cuanto a cifrado, sino en cuanto a política de identificación y a herramientas que permitan distinguir al usuario una página falsa de la original.

Las recomendaciones en estos aspectos se resumen en:

- Usar tarjetas de claves de forma que si un usuario es espiado en una transacción, no se obtenga en una sola vez acceso total a su cuenta.
- Mostrar imágenes o mensajes personalizados para cada usuario con el fin de invalidar webs scam genéricas.
- Evitar usar contraseñas cortas o solicitar partes aleatorias de una clave, pues se reduce el espacio muestral de forma alarmante y el sistema se vuelve muy vulnerable a ataques de fuerza bruta.
- Permitir identificación por DNI electrónico e ir implantándolo poco a poco en la medida de lo posible.
- Envío de claves vía SMS al usuario para confirmar transferencias bancarias.

4.4 Trabajo futuro

Este proyecto ha permitido documentar, caracterizar y descubrir lo que ocurre en el mundo del phishing a todos los nieveles, dentro de las limitaciones de material y tiempo con las que se ha trabajado.

A partir de este estudio se puede profundizar en los aspectos estudiados

4.4.1 Correo electrónico

Disponiendo de más tiempo, se puede seguir el recuento de correo no deseado recibido en nuestras direcciones dispersadas por la red, para poder comprobar si esa tendencia ascendente en la recepción llegaría a estabilizarse en algún momento.

También se pueden hacer estudios comparativos haciendo modificaciones tales como alojar direcciones en páginas de alto índice de visitas con respecto a bajo índice, hacer repartos similares para ver si existe un componente aleatorio a la hora de ser captado o es más bien previsible, etc.

4.4.2 Páginas scam

Con medios mucho mayores, se pueden realizar pruebas para comprobar cuánto tiempo pasa desde que una web falsa es denunciada hasta que se consigue cerrarla. Además de cronometrar el tiempo que tardan las autoridades en actuar, se pueden clasificar los tiempos dependiendo de en qué país están alojadas las páginas scam, pues la comunicación entre países y la rapidez de ejecución de las autoridades de los países de alojamiento presentarán grandes diferencias.

4.4.3 Malware

Las pruebas realizadas con las muestras de malware han consistido en un análisis directo. No se ha tenido tiempo ni medios suficientes como para poder comprobar qué ocurre cuando uno de los virus que quedan a la escucha recibe una orden externa. Sería necesario utilizar una máquina virtual por cada muestra de malware de este tipo, dejándola en cuarentena a la espera de que algo ocurra.

4.4.4 Muleros

En el apartado de muleros, no hemos podido ir más allá de analizar los correos electrónicos recibidos, los contratos recibidos y entablar una conversación telefónica directa con los delincuentes. Para poder dar un paso más, habría que entrar en un terreno en el que se estarían realizando actividades ilegales: recibir dinero robado para poder analizar las órdenes que recibimos de los muleros y poder estudiar el destino de este dinero y las instrucciones a seguir. Esta investigación queda en manos de la división de delitos electrónicos de la Policía.

Capítulo 5

Presupuesto

5.1 Descripción del proyecto y fases

El estudio realizado en este proyecto ha consistido en una investigación de los delitos bancarios electrónicos en la actualidad, captación de muestras de las herramientas que se usan y su posterior análisis.

Para ello se han seguido las siguientes fases:

1. **Estudio del estado del arte de los delitos bancarios electrónicos**
   Estudio del *phishing* actual, herramientas utilizadas, casos reales, consulta con expertos.

2. **Montaje de servidor y creación de direcciones de correo electrónico**
   Puesta en funcionamiento de servidor de correo, registro de dominio y esparcimiento de direcciones por la red para el estudio de vulnerabilidades en publicación de direcciones, tiempo de captación y evolución de la recepción de correo no deseado.

3. **Estudio de herramientas para realizar pruebas**
   Consulta con expertos para el estudio de herramientas del mundo del *phishing*, recopilación de herramientas para su estudio y estudio de su uso.

4. **Captación y análisis de correos phishing y muleros**
   Recopilación de correos phishing y posterior análisis de sus características principales.

5. **Captación y análisis de páginas web scam**
   Recopilación de páginas web scam y estudio profundo de sus características.

6. **Recopilación y estudio detallado de malware**
   Recopilación de malware usado en delitos electrónicos y análisis.

7. **Recopilación y estudio detallado de herramientas phishing**
   Búsqueda e investigación sobre herramientas phishing y posterior estudio y caracterización.

8. **Obtención de conclusiones**
   Obtención de conclusiones a partir de los estudios realizados y datos obtenidos en los apartados anteriores.

9. **Documentación**
   Realización de la memoria.

En el desarrollo de estas fases se han invertido 10 meses a 20 horas semanales

Horas totales: (20h/semana) x (4 semanas/mes) x (10 meses) = 800 horas

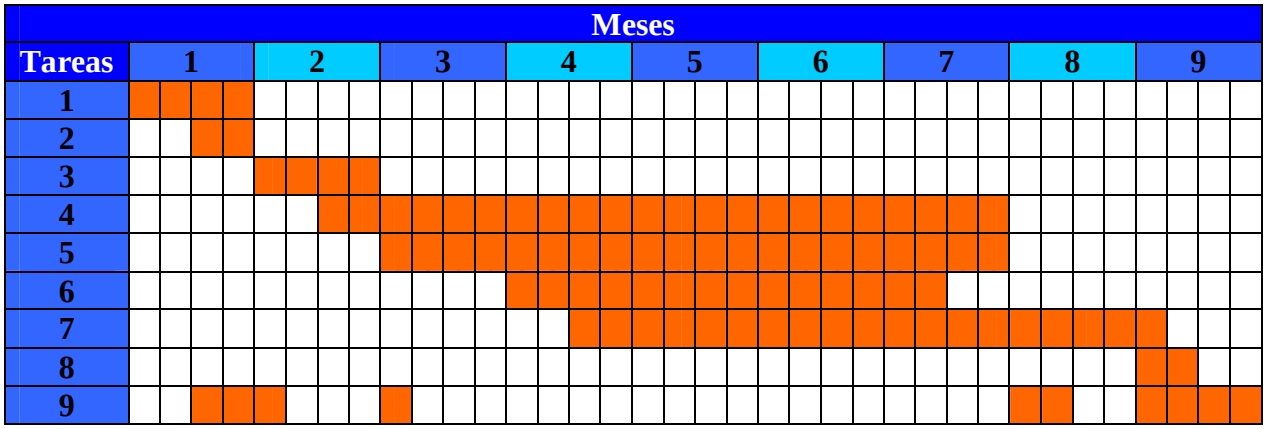


Figura 108. Diagrama de Gantt de las fases del proyecto

5.2 Presupuesto

Se realizará un cálculo de los costes económicos, desglosándolos en coste de material y coste de honorarios.

Costes software

- Windows XP: 235€
- Office XP: 150€
- Argosoft Mail Server: freeware
- VMWare Workstation: 145€
- Install Watch Pro 2.5: freeware
- Wireshark Network Analycer: freeware
- eEye Iris Professional: 345€
- Filemon: freeware
- Processexplorer: freeware

Total costes software: 875€

Costes hardware

El coste corresponde al ordenador utilizado, un AMD Athlon X2. Su coste de adquisición es de 500€. Como este equipo va a seguir siendo utilizado, su coste para el proyecto ha sido de 200€.

Costes conexión de red

Para búsqueda de información, funcionamiento de servidor de correo, acceso a páginas scam y otras actividades, ha sido necesaria una conexión de acceso a Internet, concretamente un ADSL de 10Mb.

Coste total: (19,95€/mes) x (9 meses) = 179.55€

Otros costes

Puesto de trabajo debidamente acondicionado, que conlleva unos gastos de unos 250€ mensuales. Considerando un uso de 9 meses para la realización del proyecto, el coste total del puesto de trabajo asciende a 2250€.

Total costes materiales:

Total costes materiales: 875 + 200 + 179,55 + 2250 = 3504.55€

Costes por honorarios:

El coste laboral de la hora de ingeniero superior es de 70€, sin considerarse horas extraordinarias.

(70 €/hora) x (20 horas/semana) x (4 semanas/mes) x (9 meses) = 50400€

La dirección del proyecto fue llevada a cabo por el Dr. Francisco Valera Pintor, que empleó aproximadamente 100 horas en llevar a cabo esta tarea, lo que supone un coste de 7000€.

Coste total bruto honorarios: 50400 + 7000 = 57400€

Este coste deberá ser corregido por el coeficiente reductor a aplicar según el Colegio Oficial de Ingenieros de Telecomunicación. Este coste pertenece al tramo con un coefieciente a aplicar de 0.45:

Coste total neto honorarios: 57400 * 0.45 = 25830€

Presupuesto total:

Software: 875€

Coste	*Precio (€)*
Software	875
Hardware	200
Conexión	179.55
Honorarios	25830
Total (sin IVA)	27084.55
Total (con IVA 16%)	31418

"El presupuesto total de este proyecto asciende a la cantidad de TREINTA Y UN MIL CUATROCIENTOS DIECIOCHO EUROS."

Leganés, a 18 de septiembre de 2009

El ingeniero proyectista

Fdo. Abel Lozano Prieto

Referencias

1 Argosoft Mail Server .NET. 1995-2009. Argosoft Software Design.

2 VMWare Workstation 6.0.2. ACE Edition. 1998-2007. VMWare Inc.

3 Install Watch Pro 2.5c. 1997-2000. Gavin Stark.

4 Wireshark Network Protocol Analycer 1.0.5. 1998-2008. Gerald Combs.

5 Iris Professional 5.1.0.65. 1998-2006. eEye Digital Security.

6 Filemon v7.04. Mark Russionovich & Bryce Cogswell. 1996-2006. Sysinternals.

7 Process Explorer v11.32. Mark Russinovich. 1998-2009. Sysinternals.

8 Virus Total. www.virustotal.com. 2009. Hispasec Sistemas S.L.

9 Microsoft seguridad, *Todo lo que debe saber acerca del phishing*, Mayo 2004

10 Microsoft seguridad, *What is social engineering? Social Engineering, Phishing and Email Hoaxes*, Abril 2009

11 Ron Rosenbaum, *Secrets of the Little Blue Box,* Esquire, 1971

12 Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier,* Bantam Books, 1992

13 CCN-CERT. Centro Criptológico Nacional (CCN), *Desde Rusia con una misión: robar sus datos,* Julio 2007

CAPÍTULO 5: REFERENCIAS

14 Joe Stewart, *Inside the "Ron Paul" Spam Botnet,* Secureworks.com, Diciembre 2007

15 Hispasec Sistemas, *Brasil prefiere la ingeniería social,* Enero 2008.

16 Pablo C. Caruana, *Conceptos sobre ingeniería social*, Rompecadenas.com, Junio 2002

17 Security Management Regional Congress, Kevin Mitnick, Buenos Aires, 2005

18 Carole Fennelly, *The human side of computer security*, Sunworld, Julio 1999

19 FraudWatch International Pty Ltd., *Phishing Website Methods,* 2009

20 Informa Telecoms & Media , nov 2007

21 Malware Is Poised to Outsmart the Smartphone, Zhu Cheng, Research Scientist, McAfee Avert Labs, 2007

22 Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. Octubre 2007. Inteco

23 The snooping dragon: social-malware surveillance of the Tibetan movement, Shishir Nagaraja, Ross Anderson, Computer Laboratory, University of Cambridge, Mach 2009